trg networking

PEOPLE | PROCESS | PERFORMANCE

A SAFER, STRONGER TOMORROW®

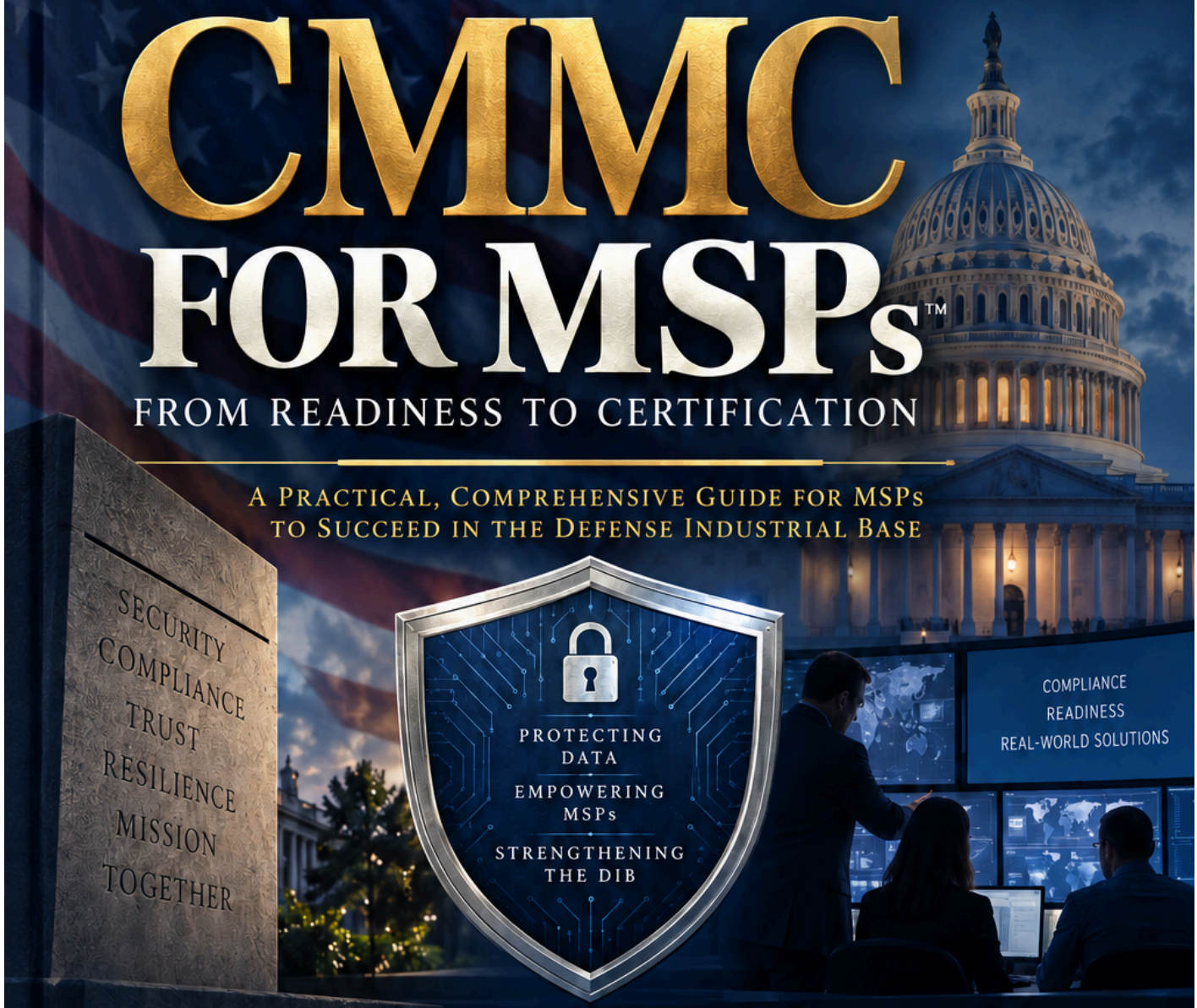
GUIDING MSPs.
STRENGTHENING DEFENSE.
SECURING AMERICA.®

"Practical Guidance for a More Secure Nation."
— DR. CHARLES EDWARDS

CMMC FOR MSPs™

FROM READINESS TO CERTIFICATION

A PRACTICAL, COMPREHENSIVE GUIDE FOR MSPs TO SUCCEED IN THE DEFENSE INDUSTRIAL BASE



PEOPLE — BUILD EXPERTISE

PROCESS — EXECUTE WITH CONFIDENCE

PERFORMANCE — ACHIEVE MEASURABLE RESULTS

COMPLIANCE — MEET TODAY'S REQUIREMENTS

PARTNERSHIP — CREATE LASTING VALUE

DR. CHARLES EDWARDS

THE CYBERSECURITY SERIES

REAL EXPERIENCE. REAL SOLUTIONS. A STRONGER TOMORROW.®

Publication Note

This book is an educational and operational reference for managed service providers and defense contractors preparing for and maintaining CMMC-related cybersecurity responsibilities.

Regulatory, contractual, assessment, and technical requirements can change. Readers should verify the current controlling contract language, Department of Defense CMMC materials, FAR/DFARS clauses, and applicable NIST publications before making a live contractual, assessment, affirmation, incident-reporting, or compliance decision.

The chapters and appendices are assembled here in full from the completed manuscript files supplied for this book.

Table of Contents

Chapter 1. CMMC: What MSPs Need to Know

Chapter 2. The MSP Role in the CMMC Ecosystem

Chapter 3. Understanding FCI and CUI

Chapter 4. CMMC Level 1 and Level 2

Chapter 5. Defining the CMMC Assessment Scope

Chapter 6. Building the CMMC Responsibility Matrix

Chapter 7. Performing the CMMC Gap Assessment

Chapter 8. Building the CMMC Remediation Roadmap

Chapter 9. Building the CMMC Evidence Package and Assessment Readiness

Chapter 10. Managing the CMMC Assessment Lifecycle

Chapter 11. Logging, Monitoring, and Security Operations

Chapter 12. Vulnerability, Configuration, and Patch Management

Chapter 13. Incident Response and Reporting

Chapter 14. Evidence: Proving That the Controls Work

Chapter 15. POA&Ms, SPRS, and Remediation

Chapter 16. Continuous Compliance and Maintaining CMMC Readiness

Chapter 17. Working with a C3PAO

Chapter 18. Assessment Day: What MSPs Should Expect

Chapter 19. After the Assessment

Chapter 20. Building CMMC into MSP Operations

Chapter 21. Implementing and Maintaining CMMC Across Three Parties

Chapter 22. The CMMC-Ready MSP Technology Stack

Chapter 23. Maintaining Certification and Continuous Readiness

Chapter 24. Building a CMMC Program from Day One

Chapter 25. MSP CMMC Case Study: From Readiness to Certification

Appendices

Appendix A. CMMC Readiness Checklist

Appendix B. MSP Scoping Checklist

Appendix C. Sample Responsibility Matrix

Appendix D. CMMC Technology Stack, Software, Licensing, and Vendor Selection Guide

Appendix E. Sample System Security Plan (SSP) Structure

Appendix F. Sample POA&M Structure

Appendix G. CMMC Assessment Preparation Checklist

Appendix H. MSP Technician Security Checklist

Appendix I. Customer Onboarding and Offboarding Checklist

Appendix J. Sample Incident Response Workflow

Appendix K. CMMC/NIST SP 800-171 Cross-Reference

Appendix L. Acronyms and Glossary

Appendix M. Operational Acceptance and Continuous Readiness Toolkit

CMMC for MSPs

From Readiness to Certification

Chapter 1

CMMC What MSPs Need to Know

By Dr. Charles Edwards

Teaching edition • September 2026

Chapter Purpose

This chapter introduces the Cybersecurity Maturity Model Certification program from the perspective of a managed service provider. It explains why CMMC exists, how the program connects to federal contracting requirements, what the three levels mean, and why an MSP can become part of a customer's assessment scope even when the MSP is not the prime contractor. The central point is simple: CMMC is not a product that an MSP installs. It is a disciplined way of showing that required safeguards are implemented, operating, and supported by credible evidence.

The chapter is written for MSP owners, technical leaders, compliance personnel, project managers, service desk managers, and technicians who support organizations in the Defense Industrial Base. It is not legal advice, and it does not replace a careful review of the applicable contract, solicitation, regulations, and official CMMC guidance.

Learning Objectives

- Explain why the Department of Defense created CMMC and what problem the program is intended to address.
- Distinguish Federal Contract Information from Controlled Unclassified Information at an introductory level.
- Describe CMMC Levels 1, 2, and 3 and identify the assessment pathway associated with each level.
- Explain how an MSP, MSSP, cloud provider, or other external service provider can affect a customer's CMMC scope.
- Recognize the difference between implementing a control and proving that the control operates as required.
- Identify the first actions an MSP should take before promising that it can support a CMMC customer.

1.1 CMMC Begins with the Information

Many MSPs first hear about CMMC when a customer forwards a questionnaire, asks whether the MSP is 'CMMC compliant,' or requests a letter stating that the customer is ready for certification. That question often arrives before anyone has determined what information the customer receives, where that information is stored, which systems touch it, or which services the MSP performs. Starting with the certification

label leads the conversation in the wrong direction. The better starting point is the information and the contractual obligation attached to it.

The Department of Defense created the CMMC program to provide a consistent method for assessing whether defense contractors and subcontractors have implemented required safeguards for Federal Contract Information, commonly called FCI, and Controlled Unclassified Information, commonly called CUI. Under 32 CFR Part 170, the program applies to contractor information systems that process, store, or transmit FCI or CUI. It also reaches systems that provide security protection for CUI systems and systems that are not logically or physically isolated from them.

That last point matters greatly to an MSP. A management server may never display a drawing, specification, or program document, yet it may administer the workstation that stores that information. A security platform may not be the customer's ordinary file repository, yet its logs, alerts, memory captures, or support attachments may contain information derived from the protected environment. Scope is therefore not limited to the obvious file server. It follows information, connectivity, administrative capability, and security dependency.

A practical rule for the MSP

Before discussing tools or certification, ask four questions: What regulated information exists? Where can it travel? Who can access or administer the systems involved? Which services protect those systems? These questions do not complete a formal scoping analysis, but they prevent the team from making an early and expensive assumption that CMMC applies only to one folder or one customer employee.

1.2 Why the Department of Defense Uses CMMC

Defense work depends on a large and diverse supply chain. Prime contractors, subcontractors, manufacturers, engineering firms, professional service companies, technology providers, and many small businesses contribute to programs that support the warfighter. Valuable information therefore resides outside government networks. Adversaries do not need to attack the largest contractor directly if a smaller supplier or service provider gives them an easier path.

For years, contractual clauses required companies to safeguard covered information. The continuing problem was not simply the absence of written requirements. The problem was inconsistent implementation and limited assurance. A company could

say that it followed a security requirement while its actual practices, configurations, records, or employee behavior told a different story. CMMC adds a structured assessment mechanism so that required practices can be examined rather than merely asserted.

For an MSP, this changes the business conversation. Security claims must be tied to observable facts. Saying that ‘MFA is enabled’ is incomplete if privileged access paths bypass MFA, emergency accounts are uncontrolled, or the MSP cannot show which users were covered during the assessment period. Saying that ‘logs are retained’ is incomplete if no one can identify the authoritative log source, retention period, review process, or tickets produced when alerts were investigated. CMMC makes these operational details visible.

1.3 The Regulatory and Contractual Chain

CMMC does not stand alone. It sits within a chain of statutes, regulations, contract clauses, security standards, and assessment methods. An MSP does not need to turn every technician into a contracting attorney, but leadership must understand the chain well enough to avoid treating a technical configuration as the entire compliance program.

Source	Primary role	Why the MSP should care
FAR 52.204-21	Provides basic safeguarding requirements for covered contractor information systems.	Its fifteen requirements form the basis of CMMC Level 1.
DFARS 252.204-7012	Addresses safeguarding covered defense information and cyber incident reporting.	It introduces important security, cloud, incident reporting, and preservation obligations for covered defense work.

Source	Primary role	Why the MSP should care
32 CFR Part 170	Establishes the CMMC program, levels, assessments, scope concepts, POA&M rules, and ecosystem roles.	It defines what is assessed and how CMMC status is achieved and maintained.
DFARS 252.204-7021	Places CMMC status and continuing compliance requirements into applicable contracts and subcontracts.	It connects the CMMC program to contract performance and flowdown.
NIST SP 800-171 Rev. 2	Provides the 110 security requirements used for CMMC Level 2 under the current rule.	MSP services often implement, support, or produce evidence for many of these requirements.
NIST SP 800-171A	Provides assessment objectives and methods for examining implementation.	It helps the MSP understand the depth of proof an assessor may seek.

A recurring source of confusion is the appearance of newer NIST publications. NIST has issued SP 800-171 Revision 3, but the current CMMC program rule incorporates SP 800-171 Revision 2 for Level 2. An MSP must work from the requirements incorporated by the applicable rule and contract, while also monitoring future changes. Using the newest-looking document without confirming contractual applicability can create a different control set from the one being assessed.

1.4 The Three CMMC Levels

CMMC uses three levels. The levels are not rankings of an MSP’s general cybersecurity maturity. They correspond to the sensitivity of the information and the assessment requirements assigned to the relevant contractor information system.

Level	Information focus	Security requirements	Typical assessment path
Level 1	FCI	15 basic safeguarding requirements from FAR 52.204-21	Annual self-assessment and annual affirmation
Level 2	CUI	110 requirements from NIST SP 800-171 Rev. 2	Either self-assessment or C3PAO certification assessment, as specified by the procurement; annual affirmation
Level 3	CUI requiring enhanced protection	Level 2 plus 24 selected requirements from NIST SP 800-172	DIBCAC assessment; annual affirmation

Level 1

Level 1 focuses on safeguarding FCI. It uses the fifteen requirements stated in FAR 52.204-21. The assessment is performed by the organization itself, and the organization must affirm continued compliance annually. Level 1 should not be dismissed as ‘easy.’ A small organization can still fail if it has unmanaged devices, shared accounts, weak physical controls, poor media disposal, or no consistent way to show that the requirements are operating.

An MSP supporting a Level 1 customer should first determine whether its services cause FCI to enter the MSP’s systems. Ticket descriptions, screenshots, backups, email, shared documentation, and remote-management scripts deserve attention. The goal is not to label every operational record as FCI. The goal is to understand the real information flow before declaring the MSP outside the boundary.

Level 2

Level 2 protects CUI and uses all 110 security requirements in NIST SP 800-171 Revision 2. Depending on the procurement, Level 2 may require a self-assessment or a certification assessment conducted by an authorized or accredited CMMC Third-Party Assessment Organization, usually called a C3PAO. The distinction is determined by the government requirement, not by the customer or MSP selecting whichever route is more convenient.

Level 2 is where MSP relationships become especially consequential. The customer may rely on the MSP for identity administration, endpoint security, logging, vulnerability management, backup, network configuration, remote access, incident response support, and maintenance. The customer cannot demonstrate many of its requirements without records or personnel from the MSP. Conversely, the MSP cannot safely promise coverage until it understands which responsibility it owns, which it shares, and which remains with the customer.

Level 3

Level 3 is intended for CUI associated with the highest-priority programs and adds selected enhanced requirements from NIST SP 800-172. The Defense Industrial Base Cybersecurity Assessment Center conducts the Level 3 assessment. Most MSPs will encounter Level 1 and Level 2 more often, but an MSP supporting highly sensitive defense work should not assume that its existing Level 2 service design will automatically satisfy Level 3 expectations.

1.5 FCI and CUI Are Related but Not Interchangeable

Federal Contract Information is nonpublic information provided by or generated for the federal government under a contract to develop or deliver a product or service. It excludes information intended for public release and simple transactional information needed to process payments. Controlled Unclassified Information is information that requires safeguarding or dissemination controls under law, regulation, or government-wide policy, but is not classified information.

The distinction affects the required CMMC level, yet the MSP should resist the temptation to classify information by intuition. A file does not become CUI because it appears sensitive, and it does not stop being CUI because the filename is ordinary. The customer should identify the contractual and program basis for the designation.

The MSP then helps translate that designation into technical locations, users, applications, data flows, and service processes.

A useful discovery session follows the information from receipt through final disposition. How does the customer receive it? Does it arrive by email, portal, secure transfer, removable media, or collaboration platform? Where is it stored? Is it synchronized to endpoints? Does it enter backup, logging, ticketing, monitoring, or disaster-recovery systems? Can MSP technicians see it during remote support? How is it transmitted to another party? How is it archived or destroyed? Each answer can change scope.

1.6 Where the MSP Fits

An MSP is an external service provider when it delivers capabilities outside the customer's organizational boundary. The exact label—MSP, MSSP, CSP, security operations provider, help desk provider, or consultant—does not decide the compliance impact. The services, access, information, and dependencies decide the impact.

The MSP may be relevant in at least four ways. First, its people may have privileged access to in-scope assets. Second, its systems may process, store, or transmit FCI, CUI, or security protection data. Third, its tools may provide security functions that the customer depends upon. Fourth, its service records may be necessary evidence during an assessment. These pathways can exist simultaneously.

MSP service	Possible scope connection	Typical evidence
Remote monitoring and management	Administrative control over endpoints and servers; scripts and automation affect configurations.	Technician access records, MFA configuration, role assignments, change tickets, script approvals
Managed identity	Creates and disables users, grants roles, enforces authentication policies.	Joiner/mover/leaver tickets, privileged role reports, MFA policies, access reviews

MSP service	Possible scope connection	Typical evidence
Managed endpoint security	Protects in-scope endpoints and may collect security protection data.	Deployment coverage, policy configuration, alert history, investigation records
Backup and recovery	Copies regulated information and supports availability and recovery.	Encryption settings, job results, restoration tests, access controls, retention settings
SIEM or SOC	Collects logs and detects activity in the protected environment.	Log source inventory, retention proof, alert rules, case records, escalation procedures
Ticketing and documentation	May contain screenshots, logs, hostnames, diagrams, credentials, or regulated content.	Data-handling rules, role permissions, retention, export controls, sample sanitized tickets

1.7 Security Protection Data Changes the Conversation

Security tools create and consume information about the protected environment. The CMMC rule uses the term Security Protection Data for data stored or processed by assets that provide security functions or capabilities. Examples can include configuration data, log data, vulnerability information, and authentication-related information. This concept prevents an organization from ignoring a security platform merely because the platform is not intended to be a CUI repository.

For MSPs, security protection data may exist in RMM platforms, SIEMs, EDR consoles, vulnerability scanners, identity services, ticketing systems, network management tools, and documentation platforms. This does not mean every MSP platform automatically becomes a CUI asset. It does mean that scoping decisions require analysis and documentation. If the customer depends on the service to satisfy a requirement, the service cannot remain a vague box labeled ‘handled by the MSP.’

1.8 Implementation Is Not the Same as Evidence

A security requirement may be implemented and still be difficult to assess because the organization cannot demonstrate it. The reverse can also occur: a policy may describe an excellent process that is not operating in the environment. A successful CMMC program aligns three things: the documented method, the technical or procedural implementation, and the evidence produced through normal operation.

Claim	Weak support	Stronger support
Privileged users use MFA	A policy statement or one screenshot from the identity portal.	Defined scope, current privileged account inventory, policy configuration, exception records, and recent authentication evidence.
Accounts are disabled promptly	A manager says HR emails the help desk.	Approved offboarding procedure, dated termination notice, closure ticket, directory record, and periodic review.
Vulnerabilities are remediated	A scanner is installed.	Authenticated scan coverage, findings, risk decisions, remediation tickets, rescan results, and trend review.
Logs are monitored	A SIEM license invoice.	Required sources, ingestion status, alert logic, analyst reviews, cases, escalation records, and retention proof.

Evidence should be a by-product of controlled operations, not a collection of screenshots created the week before an assessment. Good tickets, approvals, reports, logs, meeting records, configuration exports, and review histories make the

environment easier to operate and easier to assess. The MSP's business processes should produce this material routinely.

1.9 The Shared Responsibility Problem

Customers often believe the MSP owns every technical requirement. MSPs often believe the customer owns compliance because the customer holds the contract. Both positions are incomplete. CMMC responsibilities are distributed across people, technology, facilities, service providers, and contractual relationships. Some requirements belong to the customer, some to the MSP, and many are shared.

Consider account termination. The customer knows when employment ends and authorizes the action. The MSP may disable accounts, revoke sessions, recover equipment, remove remote access, and retain the ticket. If the customer does not notify the MSP promptly, or if the MSP closes only one of several accounts, the requirement can fail. A responsibility matrix must therefore describe more than the final task. It should identify the trigger, owner, performer, approver, evidence location, timing, exceptions, and review mechanism.

1.10 Certification Belongs to a Defined Environment

Organizations sometimes speak of becoming 'CMMC certified' as if certification attaches permanently to the company name. In practice, the status applies to a defined assessment scope and the contractor information system represented by a CMMC unique identifier in SPRS. Changes in architecture, service providers, locations, or information flow may affect that environment and must be evaluated.

An MSP should be cautious with marketing language. A product is not 'CMMC certified' merely because it has useful security features. An MSP is not automatically qualified to make every customer compliant because one environment has been assessed. The accurate statement describes the assessed organization, level, status, scope, date, and any material limitations without implying that the status transfers to another customer.

1.11 The Assessment Path in Plain Language

1. The solicitation or contract identifies the required CMMC status for the systems used in performance.
2. The organization defines the assessment scope and determines the assets, people, locations, services, and external providers that support it.

3. The organization implements the applicable requirements and documents how the environment operates.
4. The organization collects evidence through normal operations and performs an internal readiness review.
5. The required self-assessment, C3PAO assessment, or DIBCAC assessment is completed.
6. The result and applicable identifiers are recorded through the government process, including SPRS requirements.
7. An affirming official affirms continuing compliance annually, and the organization manages changes so the assessed condition remains accurate.

A conditional status may be available when limited eligible requirements remain unmet and are placed on a permitted Plan of Action and Milestones. A POA&M is not permission to postpone foundational security indefinitely. The rule restricts which requirements may be placed on a POA&M and requires timely closeout. Chapter 15 will address scoring, POA&Ms, SPRS, and remediation in detail.

1.12 A Practical MSP Scenario

Harbor Point Engineering is a fictional twenty-five-person subcontractor. It receives technical drawings and work instructions that the prime contractor identifies as CUI. Harbor Point uses Microsoft 365, local engineering workstations, a small file server, cloud backup, and an MSP named NorthStar Managed Technology.

NorthStar manages user accounts, endpoints, firewalls, backups, EDR, vulnerability scanning, and remote support. At first, NorthStar’s owner says the MSP is outside the CMMC boundary because CUI belongs to Harbor Point. A data-flow workshop produces a different picture. Backup copies leave the customer network. EDR uploads telemetry and occasionally file artifacts. Technicians can remotely control engineering workstations. Tickets contain screenshots. The documentation platform stores network diagrams and local administrator credentials. The RMM platform can deploy software and change security settings.

The correct response is not to panic or to declare every NorthStar system a CUI asset. The correct response is to classify each service and asset according to the official scoping rules, determine where CUI and security protection data exist, evaluate logical and physical separation, review external service provider requirements, and document the responsibility boundary. Harbor Point and NorthStar may decide to redesign workflows, restrict ticket attachments, isolate administrative access, move

backups, reduce technician roles, or select services that meet applicable external-provider conditions.

This scenario illustrates a theme that will appear throughout the book: good scoping is an architectural decision, not a paperwork exercise. Every system added to the boundary creates implementation, evidence, access, maintenance, and change-management obligations. Every system excluded without a defensible reason creates assessment risk.

1.13 Common MSP Mistakes

Mistake 1: Treating CMMC as a tool purchase.

A tool can support a requirement, but it cannot define the customer's scope, assign responsibilities, train users, approve risk decisions, or affirm compliance. Buying a platform without redesigning operations often creates more consoles but not more assurance.

Mistake 2: Promising compliance before discovery.

A sales proposal that guarantees compliance before reviewing contracts, information flows, architecture, and existing evidence creates legal, financial, and reputational risk. The MSP should promise a defined assessment and implementation process, not an outcome it cannot yet substantiate.

Mistake 3: Reusing generic policies without validating reality.

Policies that name nonexistent roles, tools, or review meetings are liabilities. Documentation must describe the environment that employees and technicians actually operate. Templates are starting points, not evidence of implementation.

Mistake 4: Ignoring the MSP's own platforms.

RMM, PSA, documentation, backup, security, and remote-access platforms can be central to the customer's controls. Excluding them because they are 'our tools' confuses ownership with scope relevance.

Mistake 5: Collecting screenshots at the last minute.

One-time screenshots rarely demonstrate sustained operation. Evidence should cover the selected assessment period and show repeatable processes, not a temporary configuration staged for an assessor.

Mistake 6: Assuming responsibility equals control.

A contract may say the MSP is responsible for patching, but the customer may repeatedly postpone reboots or exclude systems. The matrix, service agreement, escalation process, and evidence must address what happens when one party prevents the other from completing its responsibility.

Mistake 7: Treating all customers as one shared compliance environment.

Standardization is valuable, but evidence, scope, information, and approvals must remain attributable to the correct customer. Shared administrative platforms require careful access control and separation.

1.14 What an Assessor May Want to Understand

The assessor is not simply checking whether an MSP owns security products. The assessment examines whether applicable requirements are implemented correctly, operating as intended, and producing the desired outcome. Depending on the objective, the team may examine artifacts, interview personnel, and test or observe mechanisms.

MSP personnel should be able to explain their work plainly. A technician should know how privileged access is requested and approved. A service desk manager should know how terminations are prioritized and verified. A security analyst should know which alerts require customer escalation and where the record is kept. A technical leader should know which platforms protect the CUI environment and what happens when a platform changes.

Preparation should never coach people to memorize an artificial answer. It should ensure that the documented process and actual process are the same. When an employee cannot explain a control, that is often a useful signal that the operation depends on tribal knowledge rather than a repeatable system.

1.15 The Business Impact for MSP Leadership

Supporting the Defense Industrial Base can create a valuable specialization, but it also changes cost and risk. The MSP may need dedicated architecture, stronger identity controls, restricted technician pools, improved logging, additional supplier due diligence, formal change approval, evidence retention, contract review, and specialized training. These are not costs that should be hidden inside a conventional support plan.

Leadership should establish a service boundary and pricing model that reflect the work. The MSP must decide which platforms it will approve, which customer architectures it will support, what documentation is included, how evidence requests are handled, who participates in assessments, and what activities require separate professional services. A vague ‘CMMC package’ encourages misunderstandings. A defined service catalog creates accountability.

Contract language also deserves careful review. The MSP should not claim to certify the customer, guarantee an assessment result, or accept unlimited responsibility for decisions controlled by the customer or another provider. Agreements should describe dependencies, customer duties, change notification, evidence retention, incident coordination, subcontractors, and the consequences of refusing required remediation. Qualified legal counsel should review material commitments.

1.16 CMMC Implementation Phases and Timing

The original CMMC acquisition rollout began Phase 1 on November 10, 2025, and scheduled later phases at one-year intervals. Those dates must now be read alongside the subsequent official implementation notice. On July 13, 2026, the Department announced the immediate suspension of Phase II requirements, originally scheduled for November 10, 2026. As of this September 2026 review, readers should not treat that original Phase II date as an active deadline. The official CMMC program page and the applicable solicitation or contract should be checked before making a scheduling decision.

The original phase structure progressively expanded self-assessment, Level 2 certification, and Level 3 assessment requirements. The table below records that historical schedule; it does not establish a replacement implementation calendar following the Phase II suspension. An MSP should distinguish program-wide rollout announcements from requirements actually incorporated into a customer’s solicitation, contract, or subcontract. The suspension announcement is not, by itself, a basis for disregarding an existing contractual obligation.

The word phased should not be interpreted as permission to wait. A contractor may encounter a requirement before another company in the same industry. Existing contracts may be affected through option periods or modifications. Subcontract flowdown may also reach an organization before it sees a direct government solicitation. An MSP that waits until a customer receives an urgent requirement will

be forced to make architecture, contract, staffing, and technology decisions under pressure.

Phase	Original scheduled date / current timing note	**Practical MSP implication**
Phase 1	November 10, 2025	Expect Level 1 Self and Level 2 Self requirements; Level 2 C3PAO may also appear at DoD discretion.
Phase 2	November 10, 2026 — Phase II suspended July 13, 2026	Originally planned to broaden Level 2 C3PAO requirements. Do not use the original date as an active deadline; verify current official implementation direction and the applicable contract.
Phase 3	November 10, 2027 — original schedule	Historical rollout milestone. Confirm subsequent official implementation direction before relying on this date for planning.
Phase 4	November 10, 2028 — original schedule	Historical rollout milestone. Confirm subsequent official implementation direction before relying on this date for planning.

An MSP should incorporate the rollout into business planning. Leadership should estimate how many customers may need each level, identify assessment lead times,

decide whether a dedicated enclave service is viable, and determine whether current platforms can support the required scope. The rollout is not only a compliance calendar. It is a capacity-planning calendar.

1.17 Understanding CMMC Asset Categories

A Level 2 scoping exercise does more than list laptops and servers. The rule and official scoping guidance distinguish asset categories according to how assets interact with CUI and the security functions that protect it. The categories help the organization determine what is assessed, what must be documented, and what treatment applies. Chapter 5 will perform the detailed scoping analysis, but MSP leaders need an introductory understanding now because the categories affect service design.

CUI assets process, store, or transmit CUI. Security Protection Assets provide security functions or capabilities to the CUI environment. Contractor Risk Managed Assets can, but are not intended to, process, store, or transmit CUI because the organization has policies, procedures, and practices controlling that risk. Specialized Assets include technologies such as operational technology, Internet of Things devices, test equipment, restricted information systems, and government-furnished equipment that may require tailored treatment. Out-of-Scope Assets cannot process, store, or transmit CUI and do not provide security protections for CUI assets.

Category	Plain-language question	MSP example	Management focus
CUI Asset	Does it handle CUI?	Engineering workstation or approved CUI file repository	Implement applicable requirements and retain full assessment evidence.
Security Protection Asset	Does it protect the CUI environment?	Identity platform, firewall, EDR, SIEM, vulnerability scanner	Document the security capability, configuration, access, data, and dependencies.

Category	Plain-language question	MSP example	Management focus
Contractor Risk Managed Asset	Could it handle CUI even though that is not its intended purpose?	Corporate workstation restricted from the enclave	Document risk-based controls that prevent or limit CUI handling.
Specialized Asset	Is it a specialized technology with tailored scoping treatment?	CNC machine, OT controller, test instrument, IoT device	Inventory it, document treatment, and apply applicable risk-based safeguards.
Out-of-Scope Asset	Is it unable to handle CUI and unable to protect CUI assets?	Physically and logically separated guest kiosk	Maintain the separation that supports the exclusion.

The category is not determined by the asset owner or product label. An MSP-owned SIEM may be a Security Protection Asset for the customer environment. A customer-owned laptop may be out of scope if it is truly separated and incapable of handling CUI. A corporate workstation that could connect to the enclave may require contractor risk management even if policy says employees should not use it for CUI.

MSPs should also understand that scope is dynamic. A new integration, support workflow, identity federation, backup target, or remote access pathway can change an asset's relationship to CUI. Change-management review should therefore ask a specific question: does this change alter the CMMC assessment scope or the evidence supporting it?

1.18 External Service Providers and Cloud Services

External service providers deserve deliberate analysis because an organization may rely on them to process information or to meet security requirements. The customer remains accountable for determining that the service relationship satisfies applicable

CMMC and contractual conditions. Outsourcing the work does not outsource accountability.

A cloud service provider that processes, stores, or transmits CUI may be subject to the cloud requirements incorporated through DFARS 252.204-7012. An MSP should not reduce this analysis to a claim that a service is ‘secure’ or ‘government grade.’ The customer must verify the applicable authorization or equivalency condition, the offered service boundary, the specific configuration, data location, incident obligations, and the responsibilities retained by the customer and MSP.

The service name alone is insufficient. Commercial and government offerings from the same vendor can have different authorization boundaries, features, regions, support channels, and contractual terms. A security feature may be available but not enabled. A marketplace integration may operate outside the authorized boundary. Support personnel, diagnostic logs, connectors, or export functions may create additional data paths. The MSP should document the exact tenant, subscription, service configuration, region, integrations, and contractual commitment being used.

When an MSP provides a security function, the organization seeking assessment should document the service in its System Security Plan and Customer Responsibility Matrix. The documentation should explain what the provider does, which requirements it supports, which assets and data are involved, how access is controlled, how performance is monitored, how incidents are coordinated, and what evidence is available. A provider attestation is useful only to the extent that it addresses the service and responsibility actually relied upon.

Questions to ask every external provider

- What exact service boundary and subscription are covered by the provider’s representations?
- Will the provider process, store, or transmit CUI or security protection data?
- Which security requirements does the customer inherit, share, or retain?
- Who can administer the environment, from where, and with what authentication and monitoring?
- What logs, reports, configuration exports, and incident records will the provider make available?
- How quickly will the provider notify the customer of a suspected incident or material change?
- Which subcontractors or downstream services support delivery?

- How are data returned, preserved, and destroyed when the service ends?
- What evidence can be supplied directly to an assessor, and what requires advance coordination?

1.19 How CMMC Requirements Are Assessed

CMMC assessment is more detailed than asking whether a requirement is generally addressed. NIST SP 800-171A decomposes requirements into assessment objectives. Each objective identifies a determination that must be satisfied. A requirement that appears to be one sentence may therefore contain several distinct facts that the organization must establish.

Assessment methods include examine, interview, and test. Examine means reviewing specifications, policies, procedures, system records, configurations, plans, and other artifacts. Interview means discussing the requirement with people who have relevant responsibilities. Test means exercising or observing mechanisms and activities to determine whether they operate as intended. The assessment team selects methods and objects appropriate to the assessment.

Method	What it answers	MSP preparation example
Examine	Does the documented or recorded evidence support the objective?	Provide the current access-control procedure, role report, approval ticket, and configuration export.
Interview	Do responsible people understand and perform the process?	A service desk lead explains account provisioning, exceptions, escalation, and evidence retention.
Test	Does the mechanism or activity work as stated?	Demonstrate that an unauthorized account cannot access the enclave or that a session locks as configured.

A mature evidence package connects all three methods. The policy states what must occur. The procedure explains how staff perform it. The system configuration enforces the technical portion. Tickets and logs show that the activity occurred. Interviews confirm that personnel understand the process. Testing demonstrates that the mechanism behaves as represented.

MSPs sometimes prepare only the artifact that is easiest to export. That approach can leave assessment objectives unsupported. For example, an MFA policy screenshot does not necessarily establish that all required users, devices, protocols, and privileged pathways are covered. The MSP should map evidence to each relevant determination rather than attaching one artifact to an entire requirement and assuming the work is complete.

1.20 Building an Evidence Lifecycle

Evidence has a lifecycle. It is created, reviewed, approved, stored, protected, retrieved, retained, and eventually disposed of. Each stage should be designed. If evidence is scattered across personal mailboxes and technician desktops, the organization may be unable to demonstrate a control even though employees performed the work.

The evidence repository should identify the customer, assessment scope, requirement, evidence owner, source system, covered period, creation date, reviewer, sensitivity, retention rule, and relationship to other artifacts. The MSP should preserve native reports and exports when they provide stronger context than screenshots. Screenshots remain useful for point-in-time settings, but they should show the system, tenant, date, and relevant configuration without unnecessarily exposing secrets or unrelated customer data.

Evidence also needs quality review. A weekly vulnerability report showing hundreds of findings is not proof of effective remediation. A ticket marked complete without the affected assets or verification result may not support the objective. A policy signed three years ago may conflict with the current service. Evidence owners should examine artifacts for relevance, sufficiency, accuracy, attribution, time period, and consistency.

A practical evidence record

Field	Example
Requirement and objective	3.5.3[a] multifactor authentication is implemented for local and network access to privileged accounts
Service owner	MSP Identity and Access Team
Authoritative source	Approved identity tenant configuration and privileged role inventory
Evidence	Policy export, role report, exception register, authentication log sample, quarterly access-review approval
Period covered	July 1 through September 30, 2026
Reviewer	Customer Information System Security Manager
Storage	Customer-specific evidence repository with restricted access
Refresh trigger	Quarterly, and after material identity or remote-access change

Evidence must be protected according to its content. Configuration exports, network diagrams, vulnerability reports, authentication records, and incident tickets can provide an attacker with valuable information. The MSP should restrict evidence repositories, log access, encrypt transfers, avoid uncontrolled duplication, and establish a secure exchange method for assessors.

1.21 Governance Inside the MSP

CMMC support cannot remain a side project owned by one engineer. The service affects sales, contracting, architecture, service delivery, security operations, human resources, procurement, finance, and executive risk. Governance gives these functions a reliable way to make decisions and resolve conflicts.

The executive sponsor approves the service strategy, risk posture, investment, and claims made to customers. A CMMC program lead coordinates requirements, documentation, readiness, and assessments. The technical authority approves reference architectures and platform changes. Service owners operate controls and retain evidence. Account managers ensure that customer obligations and dependencies are understood. Legal counsel reviews contractual commitments. Human resources supports screening, training, and personnel processes. Procurement reviews downstream providers. No single title fits every MSP, but every responsibility needs a named owner.

Governance activity	Recommended cadence	Expected output
Customer scope review	At onboarding and after material change	Approved data flow, asset boundary, service inventory, and responsibility matrix
Control performance review	Monthly or quarterly based on risk	Exceptions, overdue actions, evidence gaps, and remediation decisions
Privileged access review	At least periodically and after role changes	Approved user and service-account inventory with removed access documented
Supplier review	Before use and at planned intervals	Due-diligence record, contract terms, service boundary, and change monitoring
Executive compliance review	Quarterly and before affirmation	Risk acceptance, resource decisions, material changes, and affirmation readiness

Governance should include a controlled exception process. An exception identifies the requirement, affected assets, business reason, risk, compensating safeguards if

applicable, approver, expiration date, and remediation plan. An exception cannot redefine a CMMC requirement or convert a NOT MET objective into MET. It provides visibility and management discipline while the organization determines the compliant path.

1.22 Technician Work Is Compliance Work

The daily actions of technicians frequently determine whether the documented environment remains true. A technician who creates an unapproved local administrator, moves a file into a ticket, disables a security agent to troubleshoot, or connects an unmanaged device can change the risk and evidence position. These actions may be technically convenient while undermining the assessed configuration.

Technicians therefore need task-specific guidance, not only annual awareness training. Remote support procedures should explain approved access methods, session logging, customer authorization, prohibited data movement, clipboard and file-transfer rules, emergency access, and session termination. Change procedures should identify which actions require approval and which changes trigger a scope review. Ticket templates should capture the fields needed for evidence.

A CMMC-ready service desk also knows how to recognize escalation conditions. A suspected compromise, lost device, improper CUI transmission, unauthorized account, disabled logging source, failed backup, or persistent vulnerability should not remain an ordinary ticket. The technician needs an unambiguous path to security, customer leadership, and incident coordination.

1.23 Expanding the Harbor Point Case Study

NorthStar and Harbor Point begin with a two-hour discovery session. The group includes Harbor Point’s owner, engineering manager, contract administrator, and security lead, along with NorthStar’s service manager, security architect, identity engineer, and account manager. The team places the contract and prime-contractor instructions at the center of the discussion rather than beginning with a network diagram.

They identify five CUI flows. Technical drawings arrive through the prime contractor’s approved portal. Engineers download them to designated workstations. Approved files are stored in a restricted project repository. Selected deliverables are uploaded to the prime contractor. Backup copies are created each night. During troubleshooting, technicians sometimes attach screenshots or logs to tickets.

The first four flows are expected. The fifth exposes an uncontrolled path. The ticketing platform was selected for ordinary commercial customers and has not been evaluated for CUI. NorthStar responds by prohibiting CUI attachments, adding a ticket warning, creating a secure customer exchange location, training technicians, and reviewing historical tickets. The parties assign Harbor Point to identify material as CUI and assign NorthStar to use the secure exchange when diagnostic material may contain CUI.

The team then examines privileged access. NorthStar has twenty technicians in one broad RMM role. Only six support Harbor Point, yet all twenty can initiate a session. The RMM requires MFA, but the shared emergency process is poorly documented. NorthStar creates a restricted technician group, requires customer-specific approval for elevation, rotates the emergency credential into a controlled vault, logs access, and performs a quarterly review.

Backup creates another decision. The existing backup service stores encrypted copies, but the parties cannot establish that the exact service offering meets the contractual cloud condition for CUI. NorthStar does not attempt to solve the problem with a marketing brochure. It obtains the agreement, authorization information, service boundary, data-flow documentation, encryption responsibilities, support model, and incident terms. Harbor Point’s legal and compliance advisors review the result. The parties either approve the design with documented responsibilities or migrate to an acceptable service.

Finally, NorthStar maps its services to assessment objectives. Identity evidence comes from configuration exports, privileged role reports, access reviews, and tickets. Endpoint evidence comes from deployment coverage, policy exports, alerts, and exception records. Vulnerability evidence comes from authenticated scan results, remediation tickets, risk decisions, and rescans. Backup evidence comes from job reports, restoration tests, encryption settings, and access logs. The parties schedule a monthly evidence review so gaps are found while they can still be corrected.

The expanded scenario shows why readiness requires more than producing an SSP. Each improvement changes operations: who can access the customer, where diagnostic information may go, how a service is approved, what a ticket records, and who reviews the result. Documentation follows and explains these decisions. It does not substitute for them.

1.24 A Ninety-Day Starting Roadmap

Period	Primary objective	Key actions
Days 1–30	Understand obligations and scope	Identify contracts and information; appoint owners; map services and data flows; inventory platforms, users, integrations, and providers; stop unsupported marketing claims.
Days 31–60	Establish the control model	Build the responsibility matrix; select the applicable requirements and objectives; document the current state; identify architectural and contractual gaps; prioritize high-impact remediation.
Days 61–90	Begin sustainable operation	Implement priority changes; establish evidence routines; train technicians; test core processes; conduct management review; create the longer remediation and assessment plan.

Ninety days will not make every MSP or customer ready for certification. The purpose of the roadmap is to replace uncertainty with an owned program. At the end of the period, leadership should know the applicable obligations, likely boundary,

major gaps, accountable owners, required investment, and realistic assessment timeline.

1.25 The MSP Readiness Mindset

A readiness mindset treats compliance as an operating condition. The environment should remain understandable on an ordinary Tuesday, not only during the month before an assessment. Inventory is current. Administrative access is deliberate. Exceptions are visible. Changes are approved. Evidence can be found. Personnel know their roles. When something fails, the organization records, escalates, corrects, and learns from it.

This mindset also supports security beyond CMMC. A well-maintained asset inventory helps incident response. Strong access reviews reduce account misuse. Tested backups improve resilience. Accurate diagrams speed troubleshooting. Documented responsibilities reduce delays. CMMC should therefore be integrated into service delivery rather than operated as a parallel paperwork program.

1.26 Chapter Action Plan

An MSP beginning its CMMC journey should complete the following actions before making broad compliance claims:

- Appoint an executive owner for the MSP’s CMMC service strategy and risk decisions.
- Identify current and prospective customers that perform DoD work and determine what their contracts or solicitations require.
- Conduct an information-flow and service dependency workshop for each relevant customer.
- Inventory MSP personnel, platforms, integrations, locations, and subcontractors that may touch or protect the customer environment.
- Create an initial customer/MSP responsibility matrix and identify missing owners or evidence.
- Review service agreements and marketing statements for unsupported compliance promises.
- Define rules for tickets, screenshots, remote sessions, exports, backups, logs, and customer documentation.
- Establish a repeatable evidence repository and naming convention.

- Perform an internal gap assessment against the applicable requirements and assessment objectives.
- Create a prioritized remediation roadmap that accounts for architecture, contracts, people, process, and technology.

1.27 Chapter Review

CMMC provides the Department of Defense with a consistent method for assessing whether contractors and subcontractors safeguard FCI and CUI. Level 1 is based on the fifteen basic safeguarding requirements in FAR 52.204-21. Level 2 uses the 110 requirements in NIST SP 800-171 Revision 2 and may require either a self-assessment or a C3PAO assessment. Level 3 adds selected enhanced requirements and is assessed by DIBCAC.

For an MSP, the most important early lesson is that scope follows information, administrative access, security dependencies, and connectivity. The customer's contract may drive the obligation, but the MSP's services may implement controls and produce essential evidence. CMMC readiness therefore requires a documented division of responsibility and an operating model that can be demonstrated.

The next chapter examines the MSP's role in the CMMC ecosystem in greater depth. It will distinguish MSPs, MSSPs, cloud service providers, and other external service providers; explain responsibility boundaries; and show how service design can either simplify or expand a customer's assessment scope.

Review Questions

1. Why is it better to begin a CMMC discussion with information flow rather than with a product list?

2. What problem is CMMC intended to address beyond the existence of cybersecurity clauses?

3. How do FAR 52.204-21, NIST SP 800-171 Rev. 2, 32 CFR Part 170, and DFARS 252.204-7021 relate at a high level?

4. What is the primary information focus of each CMMC level?

5. Why can an MSP platform be relevant even when it is not intended to store CUI?

6. What is the difference between implementing a requirement and producing evidence for it?

7. Give one example of a shared responsibility between a customer and its MSP.

8. Why should an MSP avoid saying that a product is ‘CMMC certified’?

9. What operational records can demonstrate that a security process is sustained?

10. Which three discovery activities should an MSP complete before promising CMMC readiness support?

Key Terms

Term	Working meaning in this chapter
C3PAO	A CMMC Third-Party Assessment Organization authorized or accredited to conduct Level 2 certification assessments.
CMMC	The Department of Defense program for assessing implementation of prescribed safeguards for FCI and CUI.
CUI	Unclassified information requiring safeguarding or dissemination controls under applicable authority.
DIB	The Defense Industrial Base—the organizations that support defense missions, products, and services.
DIBCAC	The DCMA organization that conducts specified assessments, including CMMC Level 3 assessments.
ESP	An external service provider that delivers capabilities outside the customer’s organizational boundary.

Term	Working meaning in this chapter
FCI	Nonpublic information provided by or generated for the government under a contract, excluding public and simple transactional information.
POA&M	A plan identifying corrective tasks, resources, milestones, and completion dates for eligible unmet requirements.
SPD	Security Protection Data associated with assets that provide security functions or capabilities.
SPRS	The Supplier Performance Risk System used for applicable assessment and affirmation records.

Official References

- Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. Current through September 2026. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
- Acquisition.gov. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, November 2025. https://www.acquisition.gov/dfars/252.204-7021
- Acquisition.gov. FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. https://www.acquisition.gov/far/52.204-21
- National Institute of Standards and Technology. Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, including Update 1. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
- National Institute of Standards and Technology. Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information. https://csrc.nist.gov/pubs/sp/800/171/a/final

Department CMMC program notice, July 13, 2026: Phase II suspension. Reviewed September 23, 2026. https://dodcio.defense.gov/CMMC/

Regulatory note: CMMC requirements and acquisition clauses may change. Readers should confirm the current eCFR, DFARS, solicitation, contract, and official DoD guidance before making compliance decisions.

CMMC for MSPs

From Readiness to Certification

Chapter 2

The MSP Role in the CMMC Ecosystem

By Dr. Charles Edwards

Expanded edition • September 2026

Chapter Purpose

This chapter explains where a managed service provider fits within the CMMC ecosystem and why the answer cannot be determined from the provider's business title alone. The same company may act as an MSP, an MSSP, a cloud reseller, a security operations provider, a help desk, or an external service provider depending on the service being examined. CMMC treatment follows the actual information, assets, access, and security capabilities involved.

The practical conclusion is that an MSP must understand each customer relationship at the service level. A broad statement such as "we do not store CUI" is not enough. The provider must determine whether its personnel or systems process, store, or transmit CUI or Security Protection Data; whether the customer relies on the provider to meet security requirements; and what evidence, contracts, and technical boundaries support that arrangement.

This chapter builds the foundation for Chapter 5 on scoping and Chapter 6 on the Customer Responsibility Matrix. It is intentionally detailed because mistakes made at the provider boundary affect architecture, assessment scope, contract obligations, evidence availability, pricing, and risk.

Learning Objectives

- Distinguish the practical roles of an MSP, MSSP, CSP, ESP, consultant, subcontractor, and C3PAO.
- Apply the CMMC definition of an External Service Provider to common managed services.
- Explain how CUI and Security Protection Data affect the treatment of provider services.
- Separate contractual flowdown from assessment-scope analysis.
- Identify customer, MSP, shared, inherited, and third-party responsibilities.
- Evaluate remote administration, ticketing, RMM, backup, identity, SIEM, EDR, and documentation services.
- Build a defensible service description and prepare for provider participation in an assessment.

2.1 The Ecosystem Is a Chain of Dependence

A defense contractor rarely operates every technology and security function by itself. It purchases cloud services, obtains internet connectivity, licenses software, hires

consultants, and relies on managed providers. Each dependency can affect how FCI or CUI is handled and how security requirements are implemented. The CMMC ecosystem is therefore not a simple relationship between one contractor and one assessor. It is a chain of organizations, people, platforms, facilities, and agreements.

The organization seeking assessment remains responsible for defining its environment and demonstrating that applicable requirements are met. A customer cannot answer an assessor by saying only, “our MSP handles that.” The statement identifies a dependency but does not explain the control. The customer and MSP must be able to show what the service does, what part of the requirement it supports, which systems are involved, who performs each activity, and where the evidence resides.

This dependence works in both directions. The customer controls business decisions, information identification, personnel events, contract interpretation, facilities, and many approvals. The MSP controls or operates technical services. Neither party can succeed by treating the other as a black box. Effective CMMC support begins when the parties make their dependencies visible.

2.2 Understanding the Major Roles

Role	Primary function	Important CMMC distinction
Prime contractor	Holds the direct contract with the Government.	Determines and flows applicable requirements to subcontractors based on information and work.
Subcontractor	Performs part of the prime or higher-tier subcontract.	May need its own applicable CMMC status when it processes, stores, or transmits FCI or CUI.
MSP	Operates or supports customer IT services.	May become an ESP for particular services when provider assets handle CUI or SPD.

Role	Primary function	Important CMMC distinction
MSSP	Provides managed cybersecurity capabilities.	Security platforms frequently process SPD and may be assessed as Security Protection Assets.
CSP	Provides cloud computing services.	Cloud handling of CUI invokes specific CMMC and DFARS considerations, including the exact service offering.
ESP	CMMC term for external people, technology, or facilities used for IT or cybersecurity services when provider assets process, store, or transmit CUI or SPD.	Treatment depends on data and service behavior, not the provider's marketing label.
C3PAO	Authorized or accredited organization that conducts Level 2 certification assessments.	It evaluates the OSC; it does not operate the customer's controls.
Consultant or RPO	Advises or assists with readiness.	Advice is not certification, and conflicts of interest must be managed.
DIBCAC	Government assessment organization.	Conducts specified assessments, including Level 3 certification assessments.

A company may occupy more than one role. An MSP may resell cloud subscriptions, operate a security operations center, provide compliance consulting, and hold a

defense subcontract of its own. Each relationship must be analyzed separately. The fact that a provider is a subcontractor for one engagement does not automatically make it a subcontractor for every customer, and the fact that it advises on readiness does not make it an assessor.

2.3 MSP and MSSP Are Business Descriptions

MSP and MSSP describe service models, not CMMC statuses. An MSP commonly manages endpoints, identity, networks, servers, backups, applications, and user support. An MSSP commonly manages security monitoring, endpoint detection, vulnerability management, incident support, firewalls, and related functions. Many providers perform both sets of services.

The distinction can be useful operationally, but it should not control scope analysis. A conventional help desk may handle CUI in a screenshot. A cybersecurity platform may handle no CUI but may store Security Protection Data such as logs, vulnerability results, configurations, or credentials. Both can become relevant for different reasons.

An MSP should map each service to its information and capabilities. “Managed IT” is too broad for assessment preparation. “Privileged remote administration of enclave workstations using named technician accounts with MFA and session logging” is specific enough to analyze.

2.4 The CMMC Definition of an ESP

Under 32 CFR Part 170, an External Service Provider consists of external people, technology, or facilities used to provide and manage IT or cybersecurity services on behalf of the organization. For CMMC purposes, CUI or Security Protection Data must be processed, stored, or transmitted on the provider’s assets for the provider to meet the definition.

This definition contains two tests. First, the provider supplies or manages IT or cybersecurity services. Second, the provider’s assets handle CUI or SPD. A service company that never handles either may still be contractually important, but it does not meet this specific CMMC definition for that service. Conversely, an MSP-owned platform that ingests customer logs or stores privileged credentials may meet the definition even when no one intended it to be a CUI repository.

The analysis must be factual. Examine data flows, administrative connections, temporary files, support exports, system memory, logs, credentials, configurations,

and integrations. Policies stating that CUI is prohibited are helpful only if the architecture and normal work practices make the prohibition credible.

2.5 CUI and SPD Create Different Provider Paths

Provider situation	CMMC treatment at a high level	Key MSP question
CSP handles CUI, with or without SPD	The exact cloud offering must meet the applicable FedRAMP requirements referenced by DFARS 252.204-7012.	Is the subscribed offering and boundary—not merely the vendor—acceptable for CUI?
Non-CSP ESP handles CUI	The ESP services are included in the organization's assessment scope and assessed as part of that assessment.	Can the service and provider evidence satisfy every applicable objective?
CSP or non-CSP handles SPD without CUI	The provided services are in scope and assessed as Security Protection Assets.	What security capability is provided and what SPD is created or stored?
Provider handles neither CUI nor SPD	The provider does not meet the CMMC ESP definition for that service.	What technical and procedural facts support this conclusion?

Security Protection Data includes security-relevant information used to protect the assessed environment. Examples include security configuration data, logs generated or ingested by a security asset, vulnerability information, and passwords that grant access to the environment. This is why SIEM, EDR, RMM, vulnerability, identity, and documentation platforms require careful attention.

The rule does not say that every external vendor becomes an ESP. The customer should avoid creating an unmanageable vendor list by applying the definition mechanically to organizations that neither provide relevant IT or cybersecurity services nor handle CUI or SPD. The purpose is an accurate boundary, not the largest possible boundary.

2.6 Cloud Service Providers Require Offering-Level Analysis

A Cloud Service Provider is a type of external provider, but cloud services that handle CUI have a distinct pathway. The organization must evaluate the exact product or service offering against the applicable FedRAMP condition. A vendor may have one authorized service while selling other commercial services outside that authorization boundary.

The MSP should document the tenant, subscription, region, feature set, support plan, identity model, administrative roles, network connections, encryption responsibilities, backup behavior, incident terms, and integrations. A marketplace listing or sales statement is not a substitute for this offering-level record.

The Customer Responsibility Matrix is especially important in cloud environments. The provider may secure facilities and underlying infrastructure, while the customer and MSP remain responsible for identity, configuration, endpoint security, data handling, monitoring, and user behavior. Inherited capability does not eliminate customer responsibility; it defines the portion supplied by the provider.

2.7 Contract Flowdown Is Not the Same as ESP Scoping

Two questions are often confused. The first is whether an organization is a subcontractor that must receive CMMC requirements through a subcontract or other contractual instrument. The second is whether a service provider’s assets and services are part of the customer’s assessment scope. The answers may overlap, but they are not automatically identical.

CMMC requirements apply through the supply chain to tiers that process, store, or transmit FCI or CUI in performance of the DoD contract or subcontract. The required level depends on the information flowed to the subcontractor. Separately, an ESP analysis examines IT or cybersecurity services and whether provider assets handle CUI or SPD. A provider can be relevant to assessment scope because it supplies a security capability even when the commercial relationship is not structured as performance of the defense subcontract.

The MSP should not make a unilateral legal conclusion about whether it is a subcontractor. The contracting parties and qualified counsel should review the statement of work, information exchange, performance obligations, clauses, and flowdown. The technical team supplies accurate facts about data and services; contracting professionals determine the contractual treatment.

2.8 Shared Responsibility Must Be Written

Shared responsibility means that successful implementation depends on coordinated actions by more than one party. It does not mean that responsibility is vague or that either party can assume the other will act. A strong responsibility model divides the workflow into triggers, actions, approvals, records, verification, and escalation.

Responsibility type	Meaning	Example
Customer-owned	The customer performs and proves the activity.	The customer identifies CUI and approves who needs project access.
MSP-owned	The MSP performs and provides evidence for the activity.	The MSP maintains the approved remote-access configuration and technician logs.
Shared	Both parties perform defined portions.	The customer authorizes termination; the MSP disables accounts; both verify completion.
Inherited	A provider supplies a capability documented in its service boundary.	A cloud provider supplies physical data-center protections within the authorized offering.
Third-party dependent	A separate provider performs a required function.	A SOC provider monitors alerts and sends cases to the MSP and customer.

For every shared activity, the matrix should identify the initiating event, maximum completion time, required approval, technical performer, evidence source, reviewer, exception path, and escalation contact. This level of detail prevents a control from failing in the space between two contracts.

2.8.1 A Worked Responsibility Matrix

Let us make shared responsibility concrete. Harbor Point Engineering asks NorthStar Managed Technology to administer access for its engineering enclave. A separate monitoring provider, Beacon SOC, watches security events. All three organizations are fictional. In this example, Harbor Point has 24 engineering users and NorthStar assigns three named technicians. The exact numbers, time targets, record identifiers, and review intervals used throughout these worked examples are teaching assumptions. They are not universal CMMC requirements.

Start with a request that the service desk receives frequently: an engineer needs access to a project workspace. The customer understands the business need and the information involved. NorthStar understands the technical configuration. Beacon can detect suspicious activity after access is granted, but it cannot decide whether the engineer has a legitimate business need. Writing “access control: shared” hides these differences.

Activity	Harbor Point	NorthStar	Beacon SOC
Approve access	Project owner approves purpose and duration.	Checks that approval is complete.	No business approval role.
Implement access	Confirms requested project and user.	Assigns approved role; verifies result.	Monitors relevant identity events.
Review access	Confirms continuing business need.	Exports accounts and reconciles changes.	Supplies suspicious activity cases.
Remove access	Sends authorized trigger and effective time.	Revokes access and verifies completion.	Checks for activity after revocation.
Investigate misuse	Makes business and reporting decisions.	Contains technical access under the agreed plan.	Triages alerts and preserves relevant events.

Read each row as a handoff. The matrix assigns work; the operating procedure explains how the handoff occurs. For a new user, the authorized Harbor Point project owner submits request HP-1042 through the approved channel. The request names the person, project, requested role, business justification, and access end date. A message from the new user alone does not satisfy this example's approval rule. NorthStar returns an incomplete request to the project owner instead of guessing which access is appropriate.

Following one request through completion

After verifying the approver, the technician records the approval reference, checks the identity against the customer's personnel roster, and assigns the least access needed for the approved work. The technician uses a separate named administrative account. The completion record identifies the actual role assigned and the time it became effective. Harbor Point then confirms that the engineer can perform the approved task. A separate check confirms that the engineer cannot reach an unrelated project. A successful sign-in alone would not establish that the assigned permissions are correct.

NorthStar's service owner reviews exceptions. If an application cannot enforce the approved role, the technician records the limitation and escalates it before granting broader access. A customer approval to proceed does not, by itself, establish that a security requirement is satisfied. The unresolved technical gap belongs in the remediation process, and its effect on assessment readiness must be evaluated.

Adding timing and escalation without inventing a mandate

For this fictional service, planned access changes are scheduled before the agreed effective time. Urgent revocation requests use a monitored on-call channel with a 15-minute acknowledgment target and a 30-minute containment target after receipt. These are example contractual targets, selected for the scenario. The contract must define coverage hours, authorized requesters, the start of the clock, and the escalation path when a target is missed. Actual targets require agreement based on risk, staffing, system behavior, and applicable obligations.

An acknowledgment means that someone accepted the request; it does not mean access has ended. NorthStar verifies account state, relevant sessions, tokens, application permissions, and alternate access paths. The verification method depends on the platform. Where a session cannot be immediately invalidated, the technician records that limitation and uses the agreed containment method. The closure record states what was tested, what remains, and who reviewed the result.

The completed responsibility entry therefore links four things: an authorized trigger, a named performer, a completion criterion, and a record. The broader customer responsibility matrix must connect these operational duties to applicable assessment objectives. This small table illustrates one service workflow; it is not a complete CMMC control matrix.

2.9 Evidence Ownership and Availability

A provider may operate a control while the customer remains responsible for demonstrating it. Evidence ownership must therefore be decided before the assessment. The customer needs reliable access to the records required to support its objectives, but the MSP must also protect its own confidential information and the information of other customers.

A useful agreement specifies which reports are standard, which require special preparation, how quickly they will be provided, how long records are retained, how sensitive exports are transferred, whether assessor interviews are included, and what happens after termination. If the MSP cannot produce historical evidence until an assessment request arrives, the evidence may no longer exist.

Evidence source	Customer need	MSP control
RMM activity history	Show who changed an in-scope asset and when.	Customer-filtered export, named identities, retention, and integrity controls.
Identity logs	Demonstrate authentication, privilege, and account events.	Documented source, coverage, retention, and secure export.
Security cases	Show detection, analysis, escalation, and closure.	Customer-specific cases with timestamps and analyst actions.
Vulnerability records	Show coverage, findings, decisions, remediation, and verification.	Authenticated scan scope, tickets, approvals, and rescan results.

Evidence source	Customer need	MSP control
Backup results	Show job success, failures, access, and restoration capability.	Reports, exception tickets, restore-test records, and configuration evidence.

2.9.1 Building an Evidence Package for One Access Change

Now suppose Harbor Point asks NorthStar to demonstrate how request HP-1042 was handled. The technician sends a screenshot of a user account. The screenshot is readable and shows the user enabled. Is that enough? It shows a technical state at one moment, but it does not explain who approved the access, whether the assigned permissions match the approval, or whether an unauthorized user would be blocked. We need a connected record of the decision and its implementation.

This example uses the access-control topic addressed by NIST SP 800-171 Revision 2 requirement 3.1.1 and its associated assessment objectives. The objectives examine identification and access restrictions for users, processes acting for users, and devices. The package below covers one human-user workflow only. It does not establish that the entire requirement, its other objectives, or any related requirement is satisfied. The assessment method of examining records, interviewing responsible people, and testing behavior is described in NIST SP 800-171A, June 2018, section 3.1.1. See the edition note in Official References.

Record	Example contents	What it supports
E01 Approval	HP-1042; authorized approver; user; project; role; expiry.	Business authorization for this access.
E02 Configuration	Account identifier; assigned groups; role export; capture time.	The implemented access state.
E03 Activity	Technician identity; administrative action; event time; ticket link.	Traceability of the change.

Record	Example contents	What it supports
E04 Verification	Approved task succeeds; unrelated project denied; test context.	Observed behavior of the configured access.
E05 Review	Reviewer; comparison with approval; exception disposition.	Review of the completed change.

Preparing the package so another person can follow it

NorthStar creates an index for package HP-ACCESS-1042. The index identifies Harbor Point's enclave, the service record, the request number, the collection date, and the responsible technician. For each artifact it records the source system, native identifier, collection method, relevant event period, time zone, and any filtering or redaction. The index links to the approved operating procedure and the matching responsibility-matrix entry. A reviewer should be able to follow the same account across the approval, export, event log, and test record.

A useful test record is specific. For example: "Using the approved engineering test account, project workspace A permitted the expected read operation; workspace B rejected the same operation. The test was performed at 14:10 UTC from the managed workstation listed in the record." In a real package, use the actual account and device identifiers in an appropriately protected record. A line saying "access tested successfully" leaves the reviewer unable to determine what was tested.

NorthStar retains native records alongside explanatory exports where feasible. An exported report can be easier to read, while the native record preserves detail needed for investigation. A file hash can help detect changes after collection, but it does not prove that the source record was accurate or complete. The collector still needs to explain the query, system context, and limitations. Never recreate a missing historical approval and present it as if it existed before the work occurred.

Protecting evidence without making it unusable

The evidence repository has its own access controls. NorthStar separates Harbor Point's artifacts from other customers' records and uses the approved transfer channel. The team reviews the package for CUI, credentials, security configuration,

and other sensitive material before export. Passwords, private keys, recovery codes, and live tokens do not belong in an assessment demonstration. Where redaction is necessary, retain the protected original and document what was removed. Excessive redaction can make an artifact impossible to evaluate.

The agreement identifies who retains assessment artifacts and how long, and separately identifies retention for operational logs. Those periods can differ. An example monthly evidence delivery schedule is a service arrangement, not a substitute for applicable retention obligations. NorthStar tests retrieval before promising that historical records will be available. A platform’s default retention setting may be shorter than the customer expects.

Responding when the evidence reveals a gap

During internal review, NorthStar discovers that E02 shows membership in a broad engineering group rather than the project-specific group authorized in E01. The technician corrects the membership, repeats the verification, and records when the incorrect access existed. Harbor Point and the security team evaluate whether additional investigation is warranted. The package keeps the original discrepancy and the corrective records. Replacing the original screenshot with a clean one and saying nothing would conceal the event rather than explain it.

A second gap is less visible: the package has no evidence about service identities or device authorization. NorthStar records those items as outside this package’s coverage and links them to the appropriate service records. A complete-looking folder is not the same as complete objective coverage. The customer and provider must identify which questions remain unanswered before presenting the package as assessment support.

To prepare for an interview, the project owner explains why access was approved, the technician explains how it was implemented, and the reviewer explains how the result was checked. They use the same records but speak to their own work. This is a useful readiness test: if the explanation depends on one person supplying every answer, the process may be poorly understood or insufficiently documented.

2.10 Remote Monitoring and Management

RMM platforms are powerful because they can inventory devices, run scripts, deploy software, change configuration, open remote sessions, and collect operational data.

The same capabilities that make the platform useful also make it security-critical. Compromise of the RMM can provide broad access to many customers.

For a CMMC customer, the MSP should define technician eligibility, named accounts, MFA, privileged roles, approval for elevation, session recording or logging, file-transfer rules, clipboard behavior, script approval, emergency access, device trust, source-location restrictions, and periodic access review. Shared technician accounts weaken attribution and should not be treated as an acceptable shortcut.

The MSP must also understand what the RMM stores. Hardware inventory may be ordinary operational data, while scripts can contain secrets, device notes may reveal system details, command output may include CUI, and stored credentials may be SPD. Data minimization and tenant separation should be deliberate.

2.11 PSA Ticketing and Documentation Platforms

Ticketing systems are frequent sources of uncontrolled information flow. Users paste email, attach files, upload screenshots, and describe technical problems. Technicians add logs, commands, IP addresses, diagrams, usernames, and remediation details. A statement that CUI is prohibited does not prevent accidental entry.

The MSP should provide a secure alternative for exchanging sensitive diagnostic material, display warnings at upload points, train personnel, restrict integrations, control exports, review retention, and establish a response for improper submission. Automated email ingestion deserves special attention because a customer can introduce content without opening the portal.

Documentation platforms may contain credentials, diagrams, firewall rules, recovery codes, asset lists, and customer procedures. Even when they contain no CUI, these records may be SPD. Access should be customer-specific, privileged actions should be logged, secrets should be stored in an appropriate vault, and exports should be controlled.

2.12 Identity and Privileged Administration

Identity services sit at the center of most modern MSP designs. The provider may create accounts, assign licenses, configure MFA, manage conditional access, grant administrative roles, and support federation. A mistake can affect every other control.

The customer should retain authority over who receives access and why. The MSP may implement the approved change. A complete process includes request, business

justification, approval, provisioning, verification, periodic review, role change, emergency use, and termination. Evidence must connect the human decision to the technical state.

Privileged MSP access should be separated from ordinary user activity. Named accounts, least privilege, strong MFA, monitored elevation, restricted workstations, session controls, and rapid revocation are foundational. Service accounts and application identities require ownership, credential protection, purpose, permissions, rotation, monitoring, and retirement.

2.13 Managed Security Services

EDR, SIEM, SOC, vulnerability, firewall, email-security, and incident-support services commonly process SPD. The MSP or MSSP should describe which customer assets are covered, which data are collected, where they are stored, who can access them, how long they are retained, and what occurs when the service is unavailable.

Coverage must be measurable. An EDR policy can be strong while ten endpoints are missing the agent. A SIEM can be operational while a critical log source stopped sending events weeks ago. A vulnerability platform can scan an address range while authentication fails. The provider’s responsibility includes monitoring the health of the security capability itself.

Alert handling needs a documented decision path. Define severity, triage, investigation, customer notification, containment authority, evidence preservation, ticket creation, after-hours contacts, and closure approval. A security console filled with unresolved alerts is not evidence of effective monitoring.

2.14 Backup Disaster Recovery and Business Continuity

Backup services can create complete copies of CUI and therefore demand careful design. The MSP should identify data sources, transfer method, encryption, key responsibility, storage location, administrative access, immutability, retention, deletion, subcontractors, and recovery procedures. Backup metadata and recovery credentials may also be security-sensitive.

A successful backup job proves only that a process reported success. Restoration testing provides stronger evidence that data can be recovered. Tests should define the selected system, recovery objective, authorized tester, isolation method, result,

problem resolution, and customer approval. Tests must also avoid restoring CUI into an unapproved location.

Business continuity is broader than backup. The parties must decide how identity, network access, security monitoring, communications, and required evidence will continue during an outage. A provider dependency that has no alternate process can become both an operational and compliance risk.

2.15 Subcontractors and Fourth Parties

An MSP often depends on distributors, SOC providers, backup vendors, data centers, support contractors, and software platforms. The customer may know the MSP but not the providers behind the service. These downstream dependencies can affect CUI, SPD, incident reporting, evidence, availability, and geographic or personnel restrictions.

Supplier review should occur before service activation and continue after approval. The MSP should identify the exact service, data handled, locations, access model, contractual protections, security representations, incident terms, evidence, material-change notification, and exit process. A vendor questionnaire is useful only when its answers are validated against the service actually purchased.

Contracts should require prompt notice of security incidents and material changes. If a vendor changes its architecture, authorization status, subprocessors, retention, or support model, the MSP needs enough time to evaluate the customer impact. Silent provider changes can invalidate an otherwise careful scope decision.

2.16 MSP Personnel and Work Locations

CMMC-related services are performed by people, not only platforms. The MSP should determine which employees and contractors may access the assessed environment, what screening and agreements apply, what training is required, where work may occur, and what devices may be used.

Remote work introduces questions about managed workstations, local storage, printing, visual exposure, home networks, voice assistants, removable media, and physical protection. The correct design depends on the service and information. Some MSPs use a restricted administrative workstation or virtual desktop that prevents local transfer. Whatever model is selected must be documented and tested.

Personnel changes should trigger prompt access review. Moving a technician to another team does not automatically remove customer roles. The MSP needs a joiner, mover, and leaver process that covers identity platforms, RMM, PSA, documentation, vaults, security consoles, customer tenants, VPN, emergency credentials, and physical access.

2.17 Building the MSP Service Description

A service description tells the customer and assessor what the MSP actually provides. It should be specific enough to map to requirements and evidence. It is not a marketing brochure. It is a controlled description of scope, architecture, functions, responsibilities, data, personnel, providers, and records.

- Service name, purpose, owner, and approved customer use.
- Systems, applications, facilities, integrations, and provider assets used to deliver the service.
- CUI and SPD processed, stored, or transmitted, including temporary and diagnostic data.
- Customer assets and networks connected to the service.
- Security requirements and assessment objectives supported by the service.
- Responsibilities retained by the customer, performed by the MSP, or inherited from another provider.
- Administrative access model, technician eligibility, work locations, and authentication.
- Operational procedures, monitoring, exception handling, incident coordination, and service continuity.
- Evidence produced, source system, retention period, review cadence, and delivery method.
- Subcontractors, cloud offerings, material dependencies, and change-notification requirements.

The service description should be version-controlled and reviewed after material changes. The customer’s SSP can reference it, but the two documents must remain consistent. A service description that promises session logging while the current platform does not log sessions creates an assessment and contractual problem.

2.17.1 Completed Service Record for NorthStar

A service record turns a broad promise into something the customer can examine. The following completed example brings together the access workflow and evidence package introduced earlier. It describes a deliberately limited identity-administration service. Actual technical identifiers and platform names would replace these fictional names in a customer's controlled documentation.

Service identity and boundaries

Record NS-HP-ID-01, revision 1, covers identity and privileged-role administration for Harbor Point's engineering enclave. Harbor Point's security manager owns the customer relationship. NorthStar's service manager owns delivery, with a designated backup. The customer maintains tenant HP-ENG-01. NorthStar uses three named technician identities and two managed administrative workstations, NS-PAW-01 and NS-PAW-02. The approved inventory and access roster record the actual identifiers and authorized personnel.

The service creates and disables approved user accounts, applies approved group membership, manages assigned administrative roles, reviews account-state reports, and exports supporting records. It excludes business decisions about who needs project access, classification of engineering information, engineering-file backup, and endpoint remediation. Exclusion from this service contract does not remove those activities from the customer's security program. Each excluded function needs another identified owner.

Systems and information involved

The administration console and authoritative user directory belong to Harbor Point's tenant. NorthStar maintains a restricted customer service queue, a privileged-access vault, and the two administrative workstations. Its queue records the request, approval reference, account identifier, role requested, action taken, and completion result. Its vault holds protected administrative secrets where required. Its workstations connect to the approved administrative interfaces. Beacon SOC receives selected identity events through a documented integration.

The intended workflow carries identity and security-administration information. It does not require engineering drawings, project document contents, or screenshots of CUI. Harbor Point's information owner validates that assumption for the actual fields and context. A name or project label should not be classified mechanically; the information's source, meaning, and applicable handling instructions matter. The

service record identifies Security Protection Data in credentials, security settings, and the administrative records used to protect the enclave.

Follow the information through every step. Harbor Point submits an approved request. NorthStar reviews it in the restricted queue, obtains privileged access through the approved mechanism, changes the tenant configuration, and records the result. Relevant events reach the monitoring integration. NorthStar collects evidence into the approved repository. The service record also accounts for temporary exports, browser downloads, diagnostic capture, email notifications, backups, and integration logs. A main application can be configured correctly while an overlooked notification copies sensitive content elsewhere.

Provider treatment and dependencies

For this teaching example, assume NorthStar’s own administration service is not a cloud computing offering and that the restricted provider systems handle SPD without CUI. Under the provider treatment described in 32 CFR 170.19(c)(2), the relevant service is included in scope and evaluated as a Security Protection Asset. This is a conditional application of the stated facts, not a conclusion about all MSPs or all identity services. Each actual platform and provider must be evaluated separately. Ownership of a server or use of a subscription alone does not settle whether a service is a CSP.

The customer’s cloud identity offering remains a separate dependency. The record identifies its exact service boundary and links to the provider responsibility documentation. Beacon’s monitoring service is also recorded separately, including its data intake, personnel access, escalation commitments, and evidence export. NorthStar does not treat either dependency as compliant merely because the vendor is familiar. Any additional hosted queue, vault, or evidence platform would need its own entry and analysis.

Responsibilities and operating conditions

Harbor Point approves access and maintains the authorized requester list. NorthStar implements approved changes, verifies the results, and escalates exceptions. Beacon analyzes the identity events it receives and raises cases through the agreed channel. The responsibility matrix in section 2.8.1 governs handoffs. The access-change package in section 2.9.1 defines the supporting records. The service does not grant technicians authority to approve their own standing access.

NorthStar restricts administration to the named technician team and managed administrative workstations. Ordinary browsing and email take place outside that administrative workflow. The approved design specifies authentication, privilege elevation, session controls, export restrictions, and the response to an unavailable authentication service. These conditions must be tested on the actual platform. Describing them in the service record does not make them technically effective.

Evidence delivery and verification

For the example, NorthStar delivers a customer-specific access-change register each month and supplies selected native records through the protected repository when requested. The monthly register identifies completed changes, failed requests, emergency uses, overdue approvals, and unresolved exceptions. Harbor Point’s security manager reviews the register and records follow-up actions. Retention periods are specified in the governing records schedule and contract rather than assumed from the monthly delivery frequency.

Before approving this service record, the parties walk through a test request, a rejected request, and a revocation. They verify the request channel, source of approval, actual technical permissions, resulting logs, and evidence retrieval. They also test a monitoring failure so that Beacon and NorthStar can demonstrate who notices a missing event feed. A successful account change does not establish that monitoring or evidence collection works.

Exceptions and change triggers

Revision 1 allows no engineering attachments in the service queue. If a user sends a drawing, the technician stops normal handling and follows the information-spill and incident procedures. The team evaluates all copies and dependencies rather than assuming that deletion of the ticket resolves the issue. The service record is reconsidered if normal operation actually requires CUI, if a diagnostic feature collects additional content, or if a new provider receives security data.

Other review triggers include a new integration, an added technician location, changes to the cloud offering, broader administrator permissions, altered log retention, and a new subcontracted service. NorthStar’s service owner proposes the update, Harbor Point’s security owner reviews the effect, and the technical team verifies the implemented configuration. The customer updates linked scope and SSP records as appropriate. A revision history explains why the earlier record changed.

This completed record answers a practical question: could another competent administrator understand what has been agreed and identify the evidence needed to check it? If the answer depends on undocumented knowledge, the record needs more work. It is one component of the wider scope and responsibility documentation developed in later chapters.

2.18 Contract Provisions for CMMC Services

Technical design and contract language should support one another. The agreement should identify the service boundary, applicable information, prohibited uses, customer duties, MSP duties, evidence, access, incidents, subcontractors, audit support, change notification, termination, and limitations. Qualified counsel should review material obligations.

Contract topic	Question to resolve
Information handling	What information may enter the service, and through which approved method?
Security duties	Which activities does each party perform, approve, verify, and document?
Evidence	What records are retained, for how long, and how are they delivered?
Assessment support	Are interviews, demonstrations, exports, and remediation responses included?
Incident coordination	Who notifies whom, through which channel, and within what time?
Material change	Which platform, provider, location, or process changes require notice or approval?
Termination	How are access, data return, retention, destruction, and evidence handled?
Claims and liability	What is represented, what is excluded, and who controls each dependency?

An MSP should avoid guaranteeing certification. The assessor determines the result, and the customer controls important parts of the environment. The MSP can commit to defined services, response times, configurations, evidence, and cooperation. Precise commitments are more valuable than an unlimited promise that cannot be verified.

2.19 Preparing the MSP for Customer Assessments

Provider participation should be planned. The customer and MSP should identify likely interviewees, evidence owners, demonstration environments, secure transfer methods, scheduling constraints, and approval for disclosure. The MSP should understand which statements it can make about its own operations and which decisions belong to the customer.

A readiness rehearsal can expose weaknesses. Ask the technician to demonstrate remote access. Ask the service manager to produce a termination ticket. Ask the analyst to trace an alert from ingestion to closure. Ask the identity administrator to show the current privileged population and quarterly review. The objective is not performance theater; it is confirmation that normal operations match the documents.

Evidence should be customer-specific. An assessor should not receive information about unrelated customers. The MSP may need sanitized architecture evidence, tenant-filtered exports, or a controlled demonstration. These methods should preserve sufficient detail to support the objective without disclosing unnecessary confidential information.

2.20 Architecture Patterns for MSP Supported Customers

The architecture selected by the customer and MSP strongly influences scope, cost, and operational complexity. There is no single architecture that fits every contractor. The correct design reflects the information, work processes, workforce, existing technology, contractual requirements, business continuity needs, and the organization’s ability to operate the controls consistently.

In a broad enterprise model, CUI is allowed across much of the customer environment. This can reduce friction for users, but it increases the number of assets, accounts, services, integrations, and locations that must be addressed. The MSP must maintain consistent safeguards across the larger boundary and produce evidence for a more complex system.

In an enclave model, CUI is restricted to a defined set of users, devices, applications, and services. The approach can reduce scope, but only when separation is genuine and everyday business processes support it. Users still need approved ways to receive, work with, share, print, discuss, back up, and dispose of CUI. If the enclave forces employees to bypass controls, the architecture is not sustainable.

A virtual desktop or hosted workspace can centralize processing and reduce local data storage. It does not automatically remove the endpoint from every consideration. The configuration must restrict transfer beyond keyboard, video, and mouse behavior when the organization relies on the endpoint being out of scope. Clipboard, drive mapping, printing, screenshots, downloads, browser access, and local peripherals must match the intended boundary.

Pattern	Potential advantage	Primary MSP challenge
Broad enterprise scope	Natural workflow with fewer boundaries between ordinary and CUI work.	Many assets and services require consistent implementation and evidence.
Dedicated CUI enclave	Smaller, clearer technical boundary.	Integration, user workflow, and separation must be carefully designed and maintained.
Hosted or VDI workspace	Centralized applications and data with restricted local processing.	Client configuration, transfer channels, identity, connectivity, and provider dependencies remain important.
Government furnished environment	Some capabilities and data may be supplied through government-managed systems.	The contractor must document interfaces, local responsibilities, and permitted use without assuming all duties transfer.

2.21 Segmentation and Boundary Enforcement

Segmentation is useful only when it can be explained and demonstrated. A diagram that places systems in different colored boxes is not proof of separation. The MSP should identify the enforcement points, permitted flows, identity boundaries, administrative pathways, logging, exception process, and validation method.

Network segmentation may use firewalls, access-control lists, virtual networks, security groups, or physically separate infrastructure. Identity segmentation may use separate tenants, groups, administrative accounts, conditional access, and privileged workstations. Application segmentation may use separate repositories, workspaces, or subscriptions. Administrative segmentation limits which MSP personnel and tools can control the environment.

The MSP should test the boundary from both directions. Can an ordinary corporate workstation reach the CUI repository? Can a user copy CUI into an unsanctioned collaboration platform? Can an administrator reach the enclave through a general-purpose RMM tenant? Can logs or backups cross into an unapproved service? Can a compromised corporate identity become an enclave administrator? Each pathway should have an intentional answer.

Boundary controls also require change protection. A temporary firewall rule, new single sign-on integration, troubleshooting agent, or emergency account can defeat the design. Change requests affecting the boundary should include a CMMC impact question and require review by someone who understands the approved architecture.

2.22 Commercial Model and Pricing

CMMC-ready managed services require more labor and discipline than ordinary managed support. The MSP may need restricted technician teams, dedicated administrative workstations, stronger identity, longer evidence retention, customer-specific reporting, formal configuration baselines, supplier review, documented testing, assessment interviews, and controlled change management. These activities should be recognized in the service design and price.

A low-cost bundle that assumes unlimited assessment support creates conflict later. The MSP should distinguish recurring operations from one-time readiness projects and from assessor-driven requests. Recurring services may include access reviews, evidence reports, vulnerability operations, backup tests, and control-health

monitoring. Projects may include enclave design, migration, gap remediation, SSP development support, or major platform replacement.

Assessment support also needs boundaries. The agreement should state the number of planned interviews, demonstrations, evidence exports, planning sessions, and remediation-response hours included. This does not prevent cooperation. It prevents the customer and provider from discovering during the assessment that neither budgeted for the work.

Pricing should not reward hidden shortcuts. If the compliant service requires a restricted tenant or premium cloud offering, the proposal should identify it. If after-hours incident response is required, staffing must support it. If evidence must be retained for a defined period, storage and administration must be included. Transparent pricing allows the customer to make an informed risk decision.

2.23 Provider Onboarding

Provider onboarding should occur as a controlled security change. Before access is granted, the customer and MSP confirm the approved service, information types, scope, architecture, responsibilities, contacts, personnel, platforms, connections, incident paths, evidence, and downstream providers. A signed contract without technical onboarding leaves critical assumptions unresolved.

Administrative access should not be created until named personnel, roles, authentication, approved devices, and source locations are established. The MSP should test logging and customer attribution. Emergency access should be configured, protected, and tested before an emergency occurs. Default vendor access and dormant implementation accounts should be removed or controlled.

The onboarding team should establish the baseline. Record in-scope assets, expected agents, configuration, log sources, vulnerabilities, privileged accounts, backup status, integrations, exceptions, and open remediation. Without a baseline, the parties cannot distinguish inherited problems from later service failures or demonstrate improvement.

A final onboarding review confirms that documents and reality agree. The network diagram shows the connection actually deployed. The responsibility matrix names the team performing the work. The service description names the subscribed offering. The evidence repository receives its first artifacts. Staff know how to escalate a suspected incident or improper CUI transfer.

2.24 Provider Transition and Termination

Offboarding an MSP is a security event. The outgoing provider may hold privileged identities, API tokens, vault entries, configuration copies, backups, documentation, logs, support tickets, and knowledge needed to operate the environment. A rushed transition can create loss of evidence, unmanaged systems, or continuing access.

The transition plan should identify data and configuration to be returned, evidence that must be preserved, accounts and integrations to be revoked, credentials and certificates to be rotated, agents to be removed, replacement services to be activated, open incidents and vulnerabilities to be transferred, and records the provider must retain or destroy.

Termination does not always mean immediate destruction. Contracts, incident preservation, assessment evidence, and legal obligations may require defined retention. The parties should decide what remains, why, where it is protected, who can access it, and when verified destruction occurs. The outgoing provider should supply a completion record rather than a simple statement that the account was closed.

Offboarding area	Required result
Identity and access	All provider human and machine access identified, revoked, tested, and documented.
Customer information	Approved return, transfer, retention, and destruction completed through secure methods.
Security capability	Monitoring, backup, patching, and protection continue without an unintended gap.
Evidence	Historical records remain available for the required assessment and contractual periods.

Offboarding area	Required result
Configuration	Current diagrams, inventories, baselines, rules, scripts, and recovery information are transferred.
Downstream providers	Subprocessor access and customer-specific services are terminated or reassigned.

2.25 Measuring MSP Control Performance

Service-level metrics should show whether security capabilities are operating, not merely whether the help desk is busy. Ticket closure volume may say little about CMMC effectiveness. Metrics should connect to coverage, timeliness, exceptions, verification, and risk.

Area	Useful measure	Question management should ask
Privileged access	Authorized privileged identities, overdue reviews, emergency uses, and revocation time.	Does every privileged path have an owner, need, review, and record?
Endpoint protection	Expected assets versus reporting assets, unhealthy agents, and time to restore coverage.	Which in-scope systems are not currently protected?
Logging	Required sources versus active sources, ingestion failures, retention, and review completion.	Would we notice if a critical source stopped reporting?

Area	Useful measure	Question management should ask
Vulnerability	Authenticated coverage, aging by severity, exceptions, remediation time, and rescan confirmation.	Are findings actually corrected and verified?
Backup	Job success, unresolved failures, protected systems, restore tests, and recovery results.	Can the customer recover approved data within its objectives?
Account lifecycle	Provisioning and termination time, rejected requests, orphaned accounts, and review findings.	Does the technical state follow approved personnel decisions?
Evidence	Expected artifacts received, review failures, stale records, and retrieval time.	Can we prove the control without reconstructing history?

Metrics need context and ownership. A ninety-nine percent deployment rate may sound strong, but the missing one percent could include the most sensitive engineering server. Management should review the exceptions behind the number, assign corrective action, and retain the decision record.

2.26 Provider Due Diligence Questionnaire

The following questions provide a starting point for evaluating an MSP, MSSP, CSP, or downstream provider. They do not replace verification or contract review. The customer should tailor them to the exact service and follow up when an answer is conditional, incomplete, or limited to another offering.

8. What exact legal entity, service offering, tenant, region, and support plan will deliver the service?

9. What CUI and SPD will the service process, store, transmit, generate, or temporarily access?
10. Which personnel roles can access customer systems or information, and from which locations?
11. How are privileged accounts approved, authenticated, monitored, reviewed, and revoked?
12. Which customer security requirements does the service fully perform, partially support, or leave to the customer?
13. What native evidence can be produced for each supported requirement and for what historical period?
14. Which cloud services, subcontractors, subprocessors, data centers, and support organizations are involved?
15. What security authorization, assessment, or independent reporting applies to the exact service boundary?
16. How are vulnerabilities, configuration changes, incidents, outages, and evidence gaps communicated?
17. What are the contractual notification periods, and do they support the customer's own deadlines?
18. How is customer data separated from other tenants and protected during support, backup, export, and deletion?
19. What business-continuity arrangements exist if the provider, platform, identity service, or primary region fails?
20. Which changes can the provider make without customer approval, and how is material change defined?
21. How will the provider support interviews, demonstrations, evidence requests, POA&M work, and reassessment?
22. What happens to access, data, configurations, logs, tickets, and evidence when the relationship ends?

2.27 Case Study NorthStar Defines Its Role

NorthStar Managed Technology supports Harbor Point Engineering, the fictional subcontractor introduced in Chapter 1. NorthStar initially describes itself as "the customer's MSP" and lists twelve services in a proposal. This description is commercially convenient but unusable for CMMC analysis.

The parties divide the proposal into service records. Identity administration uses the customer's cloud tenant, NorthStar technician accounts, a privileged access process,

and the MSP documentation platform. Endpoint management uses an MSP-owned RMM and EDR console. Security monitoring uses a separate SOC provider. Backup uses a cloud repository. Ticketing uses the MSP PSA. Network management uses a firewall portal and configuration backup service.

For each service, they ask whether CUI or SPD reaches provider assets. The ticketing platform is redesigned so CUI is exchanged through an approved channel. The RMM stores device configuration, scripts, and credentials, so it handles SPD. The EDR and SIEM ingest security telemetry and are Security Protection Assets. The backup service stores CUI. The identity service protects access to CUI and produces authentication records. The firewall portal stores security configuration and logs.

NorthStar then evaluates provider type. The backup platform is a CSP that handles CUI, so the exact service offering is reviewed against the applicable cloud requirements. The MSP-owned documentation and RMM services are non-CSP ESP services handling SPD and are assessed as Security Protection Assets. The SOC provider is another ESP supporting monitoring. Its responsibilities and evidence must be incorporated rather than hidden behind NorthStar’s contract.

The parties create a responsibility matrix. Harbor Point identifies users, authorizes access, classifies information, approves risk, and owns the SSP. NorthStar configures platforms, performs administration, monitors service health, manages tickets, and produces records. The SOC triages alerts and escalates cases. Shared processes include onboarding, termination, vulnerability remediation, incident response, and change management.

Finally, they update the agreements. The documents define evidence delivery, assessment interviews, notification times, subcontractors, approved work locations, material changes, and termination. NorthStar prices the work as a specialized service because the evidence and governance obligations exceed ordinary managed support. The result is not merely better paperwork. It is an operating model that each party can explain and test.

2.27.1 NorthStar Tests Its Assumptions

Let us follow NorthStar beyond the initial planning meeting. Harbor Point’s security manager asks the team to demonstrate a normal support request, an urgent access removal, and a monitoring failure. The purpose is to find gaps while the parties can still correct their operating model. This is a readiness exercise with fictional events, not a report of an actual assessment or a certification outcome.

The support ticket that changed the discussion

An engineer reports that a project application will not open and attaches a screenshot containing an engineering drawing. NorthStar's proposal says that its general service desk does not handle CUI. The screenshot shows why a proposal statement cannot be accepted without examining the workflow. The customer's information owner determines that the attachment contains CUI. The team now has an actual handling event to investigate.

NorthStar restricts access to the ticket and invokes the agreed response process. It preserves relevant records using approved methods and examines where the attachment traveled: the queue, technician browser, notification email, search index, integrations, and backup system. The team avoids casual forwarding of the image while asking for help. Harbor Point's responsible officials evaluate the reporting and contractual consequences with the incident team. The example does not assume that every improper submission automatically has the same reporting outcome.

The immediate mistake would be to delete the visible attachment and close the issue. Deletion may leave copies elsewhere, remove useful evidence, or fail to address the pathway that caused the problem. The team instead records containment, the affected systems, unresolved copies, investigation decisions, and the approved disposition of the material. It also revisits the earlier service-scope assumptions. An unexpected event needs a documented evaluation; a recurring need for CUI in support demands a redesigned and properly assessed service.

For routine support, NorthStar and Harbor Point establish an approved channel for sensitive diagnostic material. The general queue contains a restricted reference to the support case rather than a copy of the drawing. They test email submission, portal upload, technician export, and mobile access with harmless sample files. Warnings and training support the design, but the team also verifies actual permissions and transfer behavior. The approved alternative must be usable or technicians and users will invent workarounds.

The departure request that was acknowledged but not completed

Next, Harbor Point submits a planned departure request for an engineer. NorthStar disables the primary directory account at the requested time and marks the ticket complete. The internal reviewer asks whether the engineer still has an active application session or a separate project account. No one has checked. The ticket documents one action, while the business request was to end the person's access.

The technician reopens the task and follows the application inventory. NorthStar checks relevant sessions, separate identities, remote-access permissions, and any personal tokens associated with the departed user. Where a service account was sponsored by that user, the team determines whether it needs a new owner and credential change rather than disabling it blindly and interrupting production. Harbor Point validates the business dependencies. Beacon reviews available events for unexpected activity after the effective time.

The corrected procedure distinguishes the request's goal from the first technical step. The closure record identifies each access path checked, the outcome, residual limitations, and the reviewer. NorthStar adds a verification step to the responsibility matrix and tests it with a non-production account. The lesson is practical: a completed task in one console does not establish that the customer's full request has been completed.

The monitoring dashboard that stayed green

During a controlled exercise, the identity-event connector stops delivering events to Beacon. No new alerts appear. The service dashboard still shows its last successful status, and the service desk assumes that silence means normal operation. The missing capability is a check that expected data continues to arrive. The team had tested alert generation but had not tested the loss of the source itself.

Beacon and NorthStar define a source-health check based on expected event flow and connector status. The threshold is selected for the actual source, since a quiet system and a failed connector can look similar. They assign ownership for investigation, establish an escalation path, and document the effect of a monitoring gap. Harbor Point is informed when its coverage is reduced. A repeat test must demonstrate that the responsible person receives and acts on the source-health notification.

The corrective evidence includes the exercise authorization, connector interruption time, observed failure, revised monitoring configuration, notification record, investigation ticket, restoration time, and repeat-test result. The team records limitations in historical visibility. It does not fill a missing period with assumed activity. This is the difference between reporting that a monitoring tool exists and explaining whether the service operated as intended.

Reconciling the paperwork with the corrected service

After the three exercises, NorthStar updates NS-HP-ID-01, the support workflow, the responsibility matrix, and the evidence index. Harbor Point updates the corresponding

SSP and scope records where needed. Beacon updates its monitoring procedure and escalation contact list. Each document points to the same service identifiers so that a later change can be traced across the set.

Finding	Correction	Verification record
CUI entered ordinary support.	Investigate copies; implement the approved sensitive-support path.	Containment record and safe workflow tests.
Account disabled; other access unchecked.	Check all relevant identities, sessions, and application access.	Revocation checklist and tested outcomes.
Event feed failed without escalation.	Monitor source health and assign response ownership.	Failure exercise and repeat-test results.
Documents described different workflows.	Reconcile linked records and approve revisions.	Revision history and owner review.

Harbor Point’s manager asks whether these corrections mean the organization is ready for certification. NorthStar’s answer must remain bounded by the work performed. The exercises improved three workflows and produced useful evidence. The organization still needs to evaluate the full assessment scope and all applicable objectives. A service provider can explain its work, demonstrate its operation, and support assessment activities; it cannot use a successful internal exercise to promise a certification result.

The final management discussion is about remaining work. Who owns each unresolved issue? What evidence will establish completion? Does the service agreement fund the recurring reviews and response coverage? Which technical change could invalidate the assumptions? NorthStar has moved from a broad promise of support to a service that the customer can question, inspect, and test.

2.28 Common Errors at the Provider Boundary

Using the company label as the answer

“We are an MSP, not a CSP” does not determine whether provider assets handle CUI or SPD.

Assuming no CUI means out of scope

A provider handling SPD may be in scope as a Security Protection Asset.

Treating every vendor as an ESP

The CMMC definition requires the relevant service relationship and provider handling of CUI or SPD.

Relying on a vendor logo

Authorization or certification claims must be tied to the exact offering, boundary, and customer configuration.

Leaving shared controls undefined

A row marked “shared” without tasks, evidence, and timing preserves ambiguity.

Ignoring provider changes

New integrations, subprocessors, locations, or features can change scope and responsibility.

Waiting for the assessor to request evidence

Retention and export limitations may make historical proof impossible to recreate.

Guaranteeing customer certification

The MSP does not control the assessor or every customer responsibility.

2.29 Provider Decision Procedure

1. Identify the exact service, not merely the provider name.
2. Identify the people, technologies, facilities, integrations, and downstream providers used.
3. Trace CUI, temporary content, diagnostic material, credentials, logs, configurations, and vulnerability data.

4. Determine whether provider assets process, store, or transmit CUI, SPD, both, or neither.
5. Determine whether the provider is a CSP for the service being examined.
6. Apply the corresponding CMMC treatment and applicable contractual cloud requirements.
7. Document the service in the SSP, service description, architecture, inventory, and Customer Responsibility Matrix as applicable.
8. Map responsibilities and evidence to assessment objectives.
9. Review contract terms, incident coordination, material changes, and termination.
10. Reevaluate the decision after material changes and at a defined interval.

2.30 MSP Readiness Checklist

- Every CMMC-related customer has a named service owner and current scope contact.
- Services are documented individually with their systems, data, access, and dependencies.
- The MSP can identify which platforms handle CUI and which handle SPD.
- The exact cloud offerings used for CUI have been evaluated and documented.
- Technician access is named, least-privileged, strongly authenticated, reviewed, and logged.
- Ticketing and documentation workflows prevent or control unintended CUI entry.
- The MSP maintains customer-specific evidence with defined retention and secure delivery.
- Downstream providers are inventoried, reviewed, and subject to change notification.
- Customer and MSP agreements match the technical design and responsibility matrix.
- Assessment interviews and demonstrations have assigned participants and backup personnel.
- Material changes trigger CMMC impact review before implementation when practical.
- Marketing and sales language accurately describes the service without guaranteeing certification.

2.31 Chapter Review

The MSP's place in the CMMC ecosystem is determined by what it does, what its assets handle, and which security capabilities the customer relies upon. MSP and MSSP are useful business descriptions, but ESP and CSP treatment requires service-level analysis. A provider whose assets process, store, or transmit CUI or SPD can become part of the customer's assessment story even when the provider never signs the prime contract.

Cloud services that handle CUI require evaluation of the exact offering against applicable cloud conditions. Non-cloud ESP services that handle CUI are included in the organization's assessment scope. Provider services that handle SPD without CUI are assessed as Security Protection Assets. Services that handle neither CUI nor SPD do not meet the rule's ESP definition, though they may remain operationally or contractually important.

A strong MSP relationship makes responsibilities, evidence, access, providers, and change visible. The next chapter examines FCI and CUI in detail so that MSPs can recognize where protected information enters service workflows and how it moves through customer and provider systems.

Review Questions

1. Why can one company occupy several roles in the CMMC ecosystem?
2. What two conditions are central to the CMMC definition of an ESP?
3. How does SPD differ from CUI, and why does it matter to an MSSP?
4. Why is a vendor name insufficient when evaluating a cloud service?
5. How can a provider be in assessment scope without being a defense subcontractor?
6. What details should replace a responsibility matrix entry marked only as shared?
7. Why are RMM platforms especially important to provider-boundary analysis?
8. What controls can reduce accidental CUI entry into ticketing systems?
9. What should a service description contain?
10. Why should evidence delivery be addressed in the service agreement?
11. How should downstream MSP providers be evaluated?
12. What event should cause the ESP analysis to be repeated?

Practical Exercise

Select one managed service used by a hypothetical Level 2 customer. Prepare a one-page service record containing the service purpose, provider type, assets, users, data, integrations, CUI/SPD determination, supported requirements, responsibilities, evidence, downstream providers, and material-change triggers. Then explain whether the service is in assessment scope and what facts support the conclusion.

Key Terms

Term	Meaning in this chapter
CRM	Customer Responsibility Matrix describing responsibilities across the customer and providers.
CSP	External company providing cloud services based on cloud computing.
ESP	External people, technology, or facilities used for IT or cybersecurity services when provider assets handle CUI or SPD.
Inherited responsibility	A security capability supplied through a documented provider boundary.
MSP	Provider that manages customer information technology services.
MSSP	Provider that manages cybersecurity services or capabilities.
Security Protection Asset	Asset providing security functions or capabilities to the CMMC assessment scope.
SPD	Security-relevant information stored or processed by Security Protection Assets.

Term	Meaning in this chapter
Subcontract flowdown	Transmission of applicable contractual requirements to lower-tier organizations performing covered work.

Applying the Worked Examples

For the practical exercise, use NS-HP-ID-01 as a model, then choose a different managed service. Write its actual data flow, assign the handoffs, and identify three artifacts that would support the claimed operation. Explain one assumption that could change its scope treatment. A strong answer distinguishes a proposed design from a verified implementation and identifies evidence that is still missing.

Official References

- Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program, especially §§ 170.4, 170.17, 170.19, and 170.23. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
- Acquisition.gov. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. https://www.acquisition.gov/dfars/252.204-7012
- Acquisition.gov. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements. https://www.acquisition.gov/dfars/252.204-7021
- National Institute of Standards and Technology. SP 800-171 Revision 2 and SP 800-171A. https://csrc.nist.gov/publications
- Department of Defense Chief Information Officer. CMMC Program resources and guidance. https://dodcio.defense.gov/CMMC/

Regulatory note: This chapter explains the current framework for educational purposes. Organizations should confirm current regulations, acquisition clauses, official guidance, contracts, and legal obligations before making compliance decisions.

References for the worked examples

32 CFR 170.19(c)(1) and (c)(2), CMMC Level 2 asset categories and external service provider considerations. Official 2025 codification used for the illustrative provider

analysis: https://www.govinfo.gov/content/pkg/CFR-2025-title32-vol1/pdf/CFR-2025-title32-vol1-sec170-19.pdf

NIST SP 800-171A, June 2018, section 3.1.1, supplies the assessment-objective structure referenced in the access example: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf. NIST has archived this edition and superseded it with Revision 3. The example intentionally follows the Revision 2 requirement numbering used in this chapter. Select the assessment baseline specified by the applicable CMMC rules and contract; do not interchange editions solely because a newer NIST publication exists.

The NorthStar records, identifiers, operational targets, and exercise outcomes are fictional teaching examples developed for this chapter. They are not prescribed forms, required service-level targets, or a complete assessment body of evidence.

CMMC for MSPs

From Readiness to Certification

Chapter 3

Understanding FCI and CUI

Authored by Dr. Charles Edwards

September 2026

A practical guide to identifying contract information and tracing it through MSP managed environments.

Chapter topic guide

Chapter Purpose

Learning Objectives

3.1 Start with the information and the work

3.2 Understanding Federal Contract Information

3.3 Understanding Controlled Unclassified Information

3.4 Comparing the information types

3.5 Using the CUI Registry carefully

3.6 CUI Basic and CUI Specified

3.7 Reading the contract and the information together

3.8 Handling unmarked or uncertain information

3.9 Following information through its lifecycle

3.10 Email and collaboration pathways

3.11 Support tickets and screenshots

3.12 Remote support and virtual desktops

3.13 Logs and Security Protection Data

3.14 Backups and restoration

Contents continued

3.15 Paper and the physical workplace

3.16 Derived information and automated tools

3.17 Conducting a discovery workshop

3.18 Building an information register

3.19 Building a data-flow record

3.20 Worked example from receipt to delivery

3.21 When information reaches an unapproved location

3.22 Discovery tools and their limits

3.23 Turning discovery into evidence

3.24 Common mistakes and how to correct them

3.25 Practice scenarios

3.26 An MSP action checklist

3.27 Chapter review and preparation for scoping

Official References

Chapter Purpose

Before we decide which systems belong in a CMMC assessment, we need to understand the information those systems handle. That sounds straightforward until we follow a document through an ordinary workday. An engineer receives a drawing, opens it on a workstation, sends a question to a colleague, takes a screenshot for the help desk, and waits while a technician investigates. By the end of that sequence, the information may have reached several systems that were never described as engineering systems.

This chapter explains Federal Contract Information, usually called FCI, and Controlled Unclassified Information, usually called CUI. We will examine how to recognize them, how to resolve uncertainty, and how to trace their movement through an MSP-managed environment. The practical goal is to produce a defensible account of what information the customer handles and where it goes. That account becomes an input to Chapter 5 on scoping and Chapter 6 on the Customer Responsibility Matrix.

We will continue using Harbor Point Engineering, NorthStar Managed Technology, and Beacon SOC from Chapter 2. These organizations and every project, record identifier, workflow, and operational target in the examples are fictional. They give us a consistent setting in which to examine decisions. Suggested registers, interview questions, review intervals, and checklists are working methods developed for this chapter, not additional CMMC requirements.

The main point is simple: the MSP needs to understand the customer's information well enough to support the right handling decisions. Buying a security product cannot answer whether a drawing is CUI. Conversely, correctly identifying the drawing does not prove that the systems carrying it provide the required protection. We need both an informed information decision and a verified technical implementation.

How to use this chapter

Read the explanations in sequence the first time. Then return to the worked example and exercises with a customer environment in mind. Use synthetic records for practice. There is no need to place actual customer CUI in a training document to demonstrate that a workflow can protect it.

Official references appear as numbered citations near the relevant discussion and as linked entries at the end. The chapter distinguishes published requirements from recommended operational methods. Contract clauses, agency instructions, and the

applicable assessment rules control a particular engagement. The reference review date is September 19, 2026; the published edition of each cited source is identified where material.

Learning Objectives

By the end of this chapter, you should be able to explain the difference between FCI, CUI, ordinary business information, and Security Protection Data without relying on a filename or a vendor's description. You should also be able to explain why information can remain controlled when it is copied, summarized, displayed, or placed in a support record.

You will practice identifying the authority behind an information designation, documenting unresolved questions, and distinguishing a temporary protective decision from a final determination. You will trace active files and secondary copies through customer and provider systems, including email, collaboration, remote support, logging, backup, and disposal.

Finally, you will build an information register and a data-flow record, explain the limits of automated discovery, assemble useful evidence, and identify the questions that must be resolved before the assessment boundary is finalized.

3.1 Start with the information and the work

Suppose a prospective customer tells NorthStar, “We are a defense contractor, so we need CMMC.” That statement gives us a reason to begin a discussion. It does not tell us which information the company receives, what it creates, which contract requirements apply, or which systems support the work. A technician who immediately starts selecting software has moved ahead of the facts.

A more useful opening question is, “Please walk me through one piece of work from the time it arrives until you deliver the result.” The answer may begin with a purchase order, continue through an engineering package, and end with inspection results delivered to a prime contractor. Along the way, we learn who opens the package, where people work, how they ask questions, and which providers support them.

Notice that we are asking about actual work. A customer may describe its intended process accurately while overlooking an exception that happens every Friday. The project manager may use an approved workspace during the week but download a copy before traveling. The help desk may be instructed not to accept drawings while

its email gateway automatically converts every attachment into a ticket. Each exception can change the information picture.

For this reason, begin with a business conversation and then verify the technical behavior. The business owner explains the purpose and authority for handling the information. The MSP explains the systems and pathways. Neither explanation is sufficient by itself. When the two disagree, record the disagreement and investigate it rather than choosing whichever answer makes the project easier.

The first useful deliverable is therefore a short narrative of the work. For Harbor Point, it might say that designated engineers receive project packages from the prime through an approved portal, create analysis inside the engineering workspace, and return approved results through that portal. Later sections will test every part of that statement.

3.2 Understanding Federal Contract Information

FCI concerns nonpublic information provided by or generated for the Government under a contract to develop or deliver a product or service. FAR 52.204-21 excludes information the Government has made available to the public and simple transactional information needed for activities such as processing payments. The definition ties FCI to the information's purpose and contractual context. It does not make every private business record FCI merely because the business has a federal customer. [1]

Let us apply that distinction. Assume Harbor Point prepares a nonpublic progress report specifically to meet a federal contract deliverable. The report describes completed work and upcoming milestones without including controlled technical content. Under those assumptions, the report is a reasonable FCI example. If someone adds controlled technical details, we must examine whether the resulting document also contains CUI. We do not keep the original handling decision simply because the file is still called a progress report.

Now consider Harbor Point's public recruiting brochure. The company may use it to attract engineers who will eventually work on federal projects. That business connection does not make the brochure FCI. The brochure's actual content and release status matter. A separate internal staffing document created for a contract may need a different analysis.

The payment exception also requires care. A record containing only the routine details needed to complete a payment is different from an invoice package with an attached technical acceptance report. We should examine the attachments and supporting material instead of declaring that everything in the accounting folder falls within the exception. An accounting workflow can carry several information types at once.

For the MSP, the operational lesson is to avoid relying on department names. Sales, accounting, scheduling, and project management systems can all carry contract information. During discovery, ask each department what it receives from the Government or prime, what it creates for contract performance, and what it shares outside the organization. Keep examples of the decision basis without unnecessarily copying the underlying sensitive records.

3.3 Understanding Controlled Unclassified Information

CUI is unclassified information subject to safeguarding or dissemination controls grounded in applicable law, regulation, or government-wide policy. The CUI program provides a structure for identifying and handling that information. A company's preference for confidentiality does not, by itself, establish a CUI designation. The National Archives explains the program and maintains its Registry. [2, 3]

The word unclassified deserves attention. It does not mean approved for public release. At the same time, CUI is not classified national security information. A CMMC environment for CUI should never be treated as authorization to receive classified material. These are different handling situations, with different governing requirements.

Think about a drawing in two settings. One drawing appears in a manufacturer's unrestricted public catalog. Another drawing is supplied for a defense project with an identified controlled-information basis and contract handling instructions. Both may look technical. Both may contain dimensions. Their appearance alone cannot resolve their status. We need the origin, purpose, authority, and instructions that apply to the actual information.

Harbor Point's internal design notes illustrate another problem. An engineer may assume that only the material received from the prime can be controlled. However, work produced during performance can also require protection. The team must examine what the new notes reveal and the applicable contract basis. Information

does not become unrestricted merely because an employee typed it into a new document.

In practical terms, the MSP should ask the customer to identify the information owner and the person responsible for obtaining authoritative clarification. The MSP can recognize a concern, preserve the available context, and help implement protection. It should not invent a government designation because a folder looks sensitive, nor should it remove an existing restriction because the designation is inconvenient.

When teaching employees, use examples that show the reasoning. Asking people to memorize an acronym will not prepare them to recognize a controlled detail inside an email, a screenshot, or a spreadsheet. They need to understand that the information and its governing context matter across formats.

3.4 Comparing the information types

The following table is a working comparison. It helps organize questions; it does not replace a determination about a specific record. Information types can overlap, and one container can hold several kinds of information.

Information type	Basis to examine	Example under stated assumptions
Public information	Authorized public availability	An unrestricted Government publication
FCI without identified CUI	Nonpublic contract relationship and content	A routine contract progress report without controlled details
CUI	Applicable authority and contract or agency context	A controlled project drawing identified for protected handling
Company confidential information	Business policy, agreement, or other applicable obligation	An internal commercial pricing strategy unrelated to Government work
Security Protection Data	Its use in protecting the assessed environment	Administrative credentials or relevant security configuration data

Do not treat these rows as a ladder in which each higher row automatically absorbs the one below it. FCI and CUI have different definitions. In the defense-contract

setting, a CUI record may also fit the FCI definition, but the CUI program extends beyond defense procurement. Likewise, a confidential company record may require strong protection without being FCI or CUI.

Consider a shared folder containing public brochures, project schedules, controlled drawings, and administrative passwords. Giving the folder one convenient label does not explain the underlying records. Separating the records may make handling easier, but the separation needs to reflect actual permissions and workflows. Renaming four subfolders while keeping broad access to the parent directory may change very little.

For a mixed document, examine whether controlled information remains in the version being shared. A cover page saying “public summary” cannot override technical details left in an appendix. Conversely, an authorized review may establish that a separately prepared summary contains no controlled information. Preserve the decision and the exact version reviewed so that later additions do not inherit an approval they never received.

3.5 Using the CUI Registry carefully

The Registry organizes CUI categories and identifies their associated authorities. Start with the category description and follow the relevant authority rather than selecting a category because its name resembles the customer's industry. A category listing tells us what kinds of information may qualify; it does not prove that every document with a matching keyword qualifies. [3]

For Harbor Point's engineering work, Controlled Technical Information is a useful category to examine. The Registry describes technical information with military or space application that is subject to controls and identifies the relevant authority. It also distinguishes this from information lawfully available to the public without restrictions. A technical file extension alone does not establish the category. [4]

A practical research record should identify the candidate category, the relevant authority, the contract instruction, the information owner, and the unresolved question. Suppose an engineer receives a drawing with inconsistent markings. The register should preserve that inconsistency. It should not silently select whichever marking produces the simplest technical design.

NorthStar can help Harbor Point prepare a focused inquiry. Instead of asking the prime, “Is everything CUI?”, the customer can ask whether a specific drawing package and the analyses produced from it are covered, which authority and handling

instructions apply, and who can approve release or resolve a marking conflict. The question becomes easier to answer because it points to an identifiable work product.

The response should be retained in an approved location and linked to the affected records. If the answer applies to one revision or one task order, do not expand it to every future project. A useful register preserves the boundary of the answer as carefully as the answer itself.

3.6 CUI Basic and CUI Specified

CUI Basic and CUI Specified are distinguished by the underlying authority. CUI Specified applies when that authority contains particular handling controls that differ from or supplement the general CUI framework. These terms should not be taught as interchangeable with CMMC Level 1, Level 2, or Level 3. They answer different questions. The CUI Executive Agent explains that Basic and Specified are not separate protection levels. [5]

For an MSP, this means that a general statement such as “the platform supports CUI” leaves work to do. Which information category is involved? What handling conditions apply? What does the selected service actually permit? Who may access the content, including support personnel? The answers must fit the customer's information and obligations.

The Export Controlled category demonstrates why the authority matters. The Registry identifies both Basic and Specified authorities within that category. It is therefore unsafe to infer the full handling rule from the category name alone. Export authorization, recipient eligibility, and the CMMC assessment are related operational concerns, but passing one review does not resolve the others. [6]

Suppose Harbor Point wants to send a file to an outside specialist. NorthStar verifies the transfer channel and the specialist's account. Those checks establish technical conditions. Harbor Point must still establish that the recipient is authorized to receive that information and that the proposed use is permitted. A successful encrypted transfer does not answer the authorization question.

Document the approved recipients and handling conditions in a form that the service desk can apply. A technician should be able to identify the approved workflow without interpreting export regulations during a live support session. If the request falls outside that workflow, the technician needs a clear escalation contact and a way to hold the request safely while it is reviewed.

3.7 Reading the contract and the information together

A contract review and an information review support each other. The contract can identify duties and information categories, while actual samples show how those duties arise in daily work. Reading only the technical file may hide the contractual instruction. Reading only the contract may hide a new pathway created by an integration or an employee's workaround.

DFARS 252.204-7012 uses the term covered defense information. Its definition includes the relevant controlled-information basis and addresses information provided by or on behalf of DoD as well as information handled or developed by or for the contractor in contract performance. The clause should not be reduced to “only files arriving with a CUI stamp count.” [7]

During onboarding, Harbor Point's contract owner should gather the relevant contract or subcontract, task orders, incorporated requirements, information-handling instructions, and authoritative clarifications. NorthStar does not need unrestricted access to every commercial term to perform technical discovery. It needs the applicable obligations and enough context to design and explain the service accurately.

Create a record of which version was reviewed. Contracts can change, a task order can introduce different information, and a customer can add a project without changing its IT provider. An information register built during the original onboarding should therefore have a defined change trigger. “We reviewed the contract last year” does not answer whether the new project fits the existing workflow.

Where the customer and prime disagree about an obligation, keep that question with the designated contracting personnel. In the meantime, the MSP should document the technical facts and follow the agreed interim handling process. It should not translate an unresolved legal question into a confident statement that an entire environment is outside scope.

3.8 Handling unmarked or uncertain information

An absent marking should prompt examination of context, not automatic public treatment. An unexpected marking should also prompt examination rather than unquestioning expansion of a designation. The National Archives directs questions about uncertain CUI status to the originator or Government contracting activity and emphasizes following applicable contract instructions. [8]

Consider an email from the prime containing an unmarked spreadsheet. It includes measurements associated with a controlled drawing package. The engineer recognizes the relationship but cannot determine whether the spreadsheet is separately identified in the contract guidance. A good response is to limit further distribution, keep the file in the approved protective environment, and ask the designated information owner to obtain clarification.

We should describe that action accurately. The organization has made an interim protective decision. It has not necessarily completed an authoritative CUI determination. The record should say what is known, what is uncertain, who is resolving it, and which temporary restrictions apply. This prevents a temporary label from becoming an unsupported permanent conclusion.

NorthStar's ordinary ticket should contain a neutral reference such as “classification clarification request HP-023.” The underlying spreadsheet and the detailed inquiry belong in an approved location. Copying the entire spreadsheet into a general support platform just to ask whether it is sensitive would create a new handling problem before the first question is answered.

When clarification arrives, the responsible owner updates the information register and communicates the result to affected users. The MSP checks whether the technical handling needs to change and whether any earlier copies require review. If the answer is narrower than expected, retain the basis for that conclusion. If the answer confirms controlled information, assess the paths already used instead of looking only at where the file sits now.

3.9 Following information through its lifecycle

Information passes through recognizable activities: receipt or creation, use, collaboration, delivery, retention, and eventual disposition. This lifecycle is useful because it makes us look beyond the main storage location. We can ask who handles the information at each activity and which systems create additional copies.

At receipt, examine the portal, email service, transfer service, or physical media. During use, examine the application and endpoint. Collaboration may introduce messaging, shared workspaces, review tools, or external recipients. Delivery creates another transfer and an acceptance record. Retention introduces archives and backups. Disposition introduces deletion, media reuse, or destruction decisions.

The same file can exist in several lifecycle stages at once. An engineer may work on a current revision while an earlier revision remains in a backup and a delivered revision remains with the prime. Deleting the active file does not necessarily affect either of those other copies. A useful map distinguishes them rather than placing one generic “storage” box at the center.

For every location, ask whether the information is processed, stored, or transmitted there. Processing includes activities such as rendering, indexing, extracting text, or analyzing content. Storage includes temporary and historical copies as well as the official repository. Transmission includes automated integrations and provider pathways as well as a user clicking Send.

These questions are discovery prompts. They do not, by themselves, assign a final CMMC asset category. Specific scoping provisions, including the treatment of certain virtual desktop configurations, must still be applied. Here we are collecting the facts that make the later decision possible.

3.10 Email and collaboration pathways

Email can create several copies of one message before the recipient opens it. Depending on the service, a message may pass through filtering, attachment analysis, journaling, retention, or archiving. A desktop client may maintain a local copy. A mobile device may receive a preview. The MSP needs to verify which of these behaviors exists in the actual configuration.

Start by separating the message body from the attachment. An organization may use an approved portal for documents but put controlled project details in the email that announces the upload. The portal protects one part of the exchange while the message takes another route. A neutral notification can reduce that exposure, provided it still gives the recipient enough information to locate the approved item.

Collaboration tools add their own questions. Does a chat preview display the document contents? Can a guest download the file? Does a meeting recording capture a shared drawing? Are transcripts or summaries created automatically? Does a search index retain content after the visible file is removed? The answers vary by offering and configuration, so record observations rather than assuming a product name settles the matter.

For Harbor Point, NorthStar might document two separate approved uses of one collaboration platform: routine scheduling in the general tenant and controlled project

collaboration in a specifically reviewed environment. The procedures should explain how users identify the correct environment. If the two look similar, the team should test whether a user can easily share into the wrong one.

A useful validation exercise uses a synthetic document with a distinctive test phrase. Follow that phrase through the approved workflow, inspect expected notifications, and check whether prohibited recipients or locations can obtain it. Record both what the test demonstrated and what it did not test. One successful transfer cannot establish the safety of every feature in the platform.

3.11 Support tickets and screenshots

A service desk often collects exactly the material that employees should handle carefully: screenshots, error reports, sample files, and copied messages. The employee wants the technician to understand the problem. The technician wants enough context to reproduce it. Without an approved support method, both may unintentionally move information into a platform that was designed for routine support.

Suppose an engineer cannot open a controlled drawing. The engineer captures the screen, including the drawing preview, and attaches it to a ticket. The screenshot may preserve controlled content even though it is an image rather than the original drawing. The ticket may then generate an email notification, an attachment preview, and a backup. We need to investigate the entire sequence.

NorthStar should make the safe method practical. An initial ticket can identify the affected application, the time of the error, and a neutral project reference. If the technician needs to see controlled content, the work can move to an approved support session or protected evidence location. The ticket links to an authorized reference without reproducing the content.

Sanitizing a screenshot requires more than drawing a black rectangle over the visible area. The reviewer must consider whether the method permanently removes the information and whether other visible details or embedded content still disclose it. For routine troubleshooting, reproducing the error with a synthetic file is often easier to verify than editing a real customer image.

Train technicians to recognize the situation without blaming the user. An employee who reports an accidental attachment quickly gives the organization an opportunity to contain it. The response should preserve the necessary facts, limit access, and use the

incident process. Quietly deleting the attachment and closing the ticket can hide the distribution history and make later investigation harder.

3.12 Remote support and virtual desktops

Remote access requires a precise description of what crosses the connection. A technician may send keyboard and mouse input while receiving a screen display. The same product may also support clipboard synchronization, file transfer, drive mapping, printing, recording, or diagnostic collection. An assessment of one configuration should not be reused for another without checking those features.

A general statement that “remote viewing always brings the technician's device into the CUI boundary” would be too broad. The published Level 2 scoping rule includes a specific out-of-scope provision for an endpoint hosting a VDI client configured to permit no CUI processing, storage, or transmission beyond keyboard, video, and mouse. Applying that provision requires the actual conditions to be satisfied. It is not a blanket exception for every remote-support product or connection. [9]

For Harbor Point, NorthStar should record which remote method is approved, where the technician authenticates, which redirection features are disabled, and how those restrictions are verified. If a session can produce a local recording or permit copying a file, the review needs to address that behavior explicitly.

Also separate the content path from the administration path. A technician's workstation may have access to credentials, management consoles, or security configuration data even if a particular viewing session fits a narrow content-handling arrangement. That other role still needs analysis. One favorable conclusion about the screen connection does not describe the technician's entire workstation or toolset.

Test routine work and troubleshooting exceptions. A technician may enable a feature temporarily to solve a difficult problem and forget to reverse it. The change record should show the authorization, exact change, handling implications, and verification after restoration. An approved baseline has value only when the team can recognize and manage deviations.

3.13 Logs and Security Protection Data

Security tools often collect data about the environment rather than the business documents themselves. Chapter 2 introduced Security Protection Data, or SPD, and explained why provider services can matter even without CUI. For this chapter, the

important discovery question is what the tool actually collects and whether the collected content includes customer information beyond the intended security metadata.

A login event with a user identifier, source address, result, and timestamp differs from a diagnostic package that includes command output, document fragments, or a memory capture. Calling both “logs” hides a material difference. NorthStar should inspect representative event fields and collection settings rather than accepting a broad statement that the monitoring service never receives customer content.

File paths and command lines deserve attention because they may reveal project names or data inserted into a command. They are not automatically CUI in every setting. Their status depends on what they disclose and the applicable basis. The practical response is to review the data fields and their use, then document whether content minimization or additional handling is needed.

Beacon SOC may need sufficient detail to investigate suspicious activity. Removing every useful field can weaken monitoring. NorthStar and Harbor Point should therefore agree on the information needed for the service, the approved destination, access restrictions, and how exceptional evidence is transferred. A normal alert feed and a forensic evidence transfer may require different procedures.

Keep the tool's purpose and its payload separate in the record. A system can provide security protection while also collecting CUI. Discovering controlled content in a feed should trigger review of the provider pathway and the affected configuration. It should not be dismissed because the product was purchased under a security budget.

3.14 Backups and restoration

A backup is another copy of the information. The MSP needs to know what enters the backup, where it is stored, who can restore it, and where restoration can place the recovered data. A dashboard showing successful jobs answers only one of those questions.

Suppose Harbor Point keeps its active engineering files in an approved workspace, but NorthStar restores a failed project folder into a general technician share for inspection. The original storage decision does not authorize the restore destination. Recovery procedures should name an approved destination and explain how the technician verifies the restored permissions before making the data available.

Encryption is part of the technical analysis, but it should not be treated as a declaration that the information is no longer CUI or that a provider is automatically outside scope. Examine the service arrangement, key handling, access, and applicable requirements. When covered defense information is handled by an external cloud provider, DFARS 252.204-7012 includes a FedRAMP Moderate equivalence condition and specified incident-related duties. The exact offering and agreement require review. [7]

Retention creates another practical issue. A file removed from the active workspace may remain in immutable or historical backups until scheduled expiration. Document that residual location and the restrictions on restoration. Do not promise immediate eradication if the service cannot perform it, and do not improvise a destructive cleanup that violates a preservation obligation.

A restoration exercise should use synthetic data when the purpose is to test workflow and permissions. If an actual recovery requires customer information, conduct it through the approved process. Record the source, destination, operator, authorization, result, and treatment of temporary copies. The record should show that the recovery preserved the intended handling conditions as well as recovering the bytes.

3.15 Paper and the physical workplace

A data-flow review should include the moment information leaves the screen. A user may print a drawing for a production discussion, carry it to another room, mark it by hand, and scan it back into the project record. Each action can introduce a location, device, or person that is absent from the logical network diagram.

For Harbor Point, ask where project printing is permitted and how users collect output. Examine the actual printer and workflow. Does a queued job remain available for reprinting? Does the device retain a scanned image? Where does scan-to-email send the result? The answer depends on the equipment and configuration and should be verified rather than inferred from the device's location.

Physical access also affects routine support. A technician repairing a workstation may encounter a printed drawing on the desk even when the ticket concerns an unrelated application. The support procedure should tell the customer how to prepare the workspace and tell the technician what to do if controlled material is present unexpectedly.

Remote work requires the same attention. An employee may use the correct application while displaying a document where unauthorized people can see it. A home printer can create an uncontrolled paper copy. The customer's rules need to translate information-handling expectations into specific permitted activities that employees can follow.

Disposition completes the physical path. Track media or paper through the approved destruction or sanitization process, with records appropriate to the applicable requirements. A document disappearing from a desk is not evidence that it was disposed of correctly. The MSP's role may be limited, but the responsibility should be assigned so that the gap is visible.

3.16 Derived information and automated tools

Information can move without the original file moving. An engineer may quote a controlled tolerance in a chat, paste results into a presentation, or summarize a technical limitation in a support request. The recipient receives the substance through a new format. The review must therefore examine what the new material reveals.

The same reasoning applies to automated extraction and analysis. An optical character recognition service may create searchable text from an image. A search feature may create an index. An AI assistant may receive a prompt, uploaded file, retrieved passage, or generated response. These are separate processing and storage questions, even when the user sees one convenient button.

For a proposed AI feature, NorthStar should identify the exact service offering, the information sent to it, the retention and access behavior, any additional providers, and the approved contractual use. A setting that prevents model training addresses one concern. It does not establish every condition required for handling the customer's information.

A useful pilot uses synthetic data and a narrowly described task. For example, the team can test whether the assistant produces a useful maintenance summary from a fictional fault report. If the pilot is successful, the customer still needs to authorize the real information flow and the MSP needs to verify the production configuration. A useful demonstration is not the same as an approved handling arrangement.

Also review the output. A generated summary may reproduce controlled details from its input. It should not be treated as public merely because software composed the sentences. If an authorized reviewer prepares a version for broader distribution, retain

the reviewed version and the release basis. Later edits require attention because they can reintroduce information that was removed.

3.17 Conducting a discovery workshop

A productive workshop brings together people who understand the contract, the work, and the technology. For Harbor Point, that includes the contract owner, an engineering representative, an information or security owner, and NorthStar's service lead. Beacon may join the portion dealing with monitoring and evidence. Participation should be purposeful; a large meeting does not compensate for the absence of the person who knows how the work actually happens.

Begin with one recent, representative workflow. Ask the engineer to describe how a project package arrives and what happens next. Use safe demonstrations or neutral references rather than projecting actual controlled material to an unnecessarily broad audience. Record the normal path first, then ask about exceptions, urgent work, remote work, and outages.

The interviewer should ask concrete follow-up questions. “Where do you save it before uploading?” is more useful than “Do you follow policy?” “What does the technician receive when you click Report a Problem?” can reveal an automatic attachment. “Who can open the backup console?” can reveal a provider dependency that the business team never sees.

After the meeting, compare the narrative with configuration and records. The engineer may believe downloads are blocked while a local synchronization client remains active. The service lead may believe recording is disabled while one support group uses a different profile. Record these differences as findings with owners and follow-up actions.

Close the workshop with a short statement of what is established and what remains unresolved. Avoid filling gaps with assumptions merely to finish the diagram. An honest unresolved question has an owner, a next step, and a temporary handling decision. An unrecorded assumption can survive until the assessment or an incident exposes it.

3.18 Building an information register

An information register connects a business record to its handling decision. It is not simply an inventory of file extensions. A useful entry explains what the information

is, why the organization handles it, the basis for its status, and the approved workflow. The register can refer to collections or record types when that is practical; it does not need one row for every file.

For our example, Harbor Point creates register entry IR-017 for a fictional controlled engineering package. The entry refers to the project's contract guidance and the customer's retained clarification. We assume those documents establish the CUI basis for this teaching scenario. We are not assigning a real-world category to unseen technical information.

Register field	Fictional entry IR-017
Information and purpose	Engineering package and associated analysis for Project Alder
Determination basis	Applicable project instruction and retained customer clarification
Status and owner	CUI for this scenario; Harbor Point engineering information owner
Approved locations	Reviewed transfer portal, engineering workspace, approved backup service
Permitted recipients	Named project personnel and specifically authorized external recipients
Support method	Neutral ticket reference and approved protected support workflow
Open question	Whether one diagnostic export contains controlled content
Review trigger	New project instruction, recipient, tool, or material workflow change

The register should also capture the date and version of the decision record and the person responsible for maintaining it. Where the decision is provisional, say so. A register that conceals uncertainty may look complete but is less useful than one that identifies the missing answer.

Keep the register itself appropriately protected. It can reveal customer relationships, projects, architecture, and handling weaknesses. Record enough detail to support decisions without copying technical content that belongs in a separate approved repository. A neutral identifier often makes cross-referencing possible without reproducing the sensitive material.

The MSP should agree with the customer on maintenance responsibilities. Harbor Point owns the business and information determination. NorthStar updates the technical locations and workflows it operates. Changes that affect both require a coordinated review. Otherwise, the information owner may approve a new process while the register continues describing last month's architecture.

3.19 Building a data-flow record

A useful data-flow record identifies a source, destination, purpose, content, transfer mechanism, responsible party, and verification method. It should also identify secondary copies. An arrow labeled “secure” does not tell us what moves or where the evidence comes from.

For each important flow, distinguish intended behavior from observed behavior. NorthStar may intend for a notification to contain only a neutral reference. The test should verify the actual email, including its preview and attachment behavior. If the message includes a document title that discloses controlled information, the record needs to reflect that result.

Flow	Source and destination	What to verify
F01 Receipt	Prime portal to engineering workspace	Authorized recipient, approved transfer, temporary download behavior
F02 Analysis	Workspace to engineering application	Working copies, autosave, export paths, access restrictions
F03 Support	Engineer to NorthStar support workflow	Neutral ticket content and approved handling of needed evidence
F04 Monitoring	Security tools to Beacon	Event fields, collection settings, exceptional content transfers

Flow	Source and destination	What to verify
F05 Backup	Workspace to backup service	Included data, destination, permissions, restore path
F06 Delivery	Workspace to prime portal	Approved version, recipient, transfer and acceptance record

These flows describe the example, not a universal architecture. A different customer might use an entirely different approved path. The value lies in the method: every transfer has enough detail to examine and a person who can explain it.

A network diagram can show connectivity and boundaries, while the flow record explains the information crossing them. Keep the identifiers consistent so a reviewer can move between the two. If the diagram names a transfer service and the register names a different product, resolve the discrepancy rather than assuming the reader will understand the relationship.

3.20 Worked example from receipt to delivery

Let us now follow one complete job. Harbor Point receives a fictional engineering package for Project Alder. The customer has already established the CUI basis and approved the handling instructions. NorthStar administers the reviewed engineering environment. Beacon monitors its security events. We will focus on information movement, not claim that the example satisfies every CMMC requirement.

Receiving the package

The authorized engineer receives a neutral notification that a package is available in the prime's portal. The notification contains a project reference but no controlled drawing content. The engineer signs in through the approved method and brings the package into the engineering workspace using the documented transfer procedure.

NorthStar verifies where temporary files are created during that transfer. If the browser downloads to an endpoint folder before the file is moved, that folder is part of the observed path. The team should not draw a direct portal-to-workspace arrow when the actual process includes another location. The receipt record identifies the package revision and its approved destination.

Creating the analysis

The engineer opens the package in the approved application. The application creates an autosave copy and a preview. NorthStar's application review has identified both locations. The analysis produces a new report that includes controlled details from the source. Harbor Point applies its approved handling instructions to that report instead of assuming a newly created file is unrestricted.

The engineer then asks a colleague to review the calculations through the approved workspace. The colleague receives access appropriate to the task. The review record identifies the version examined, because a later revision may contain different information or conclusions. Version discipline supports both the engineering work and the information-handling record.

Resolving a support problem

The engineer encounters a rendering error. The first ticket contains the application name, error time, and reference IR-017. It does not contain a drawing screenshot. NorthStar begins with a synthetic file to determine whether the issue is general. When the problem cannot be reproduced, the technician uses the approved protected support method.

The support record shows the session authorization and diagnostic steps. If a diagnostic export is needed, the technician pauses to inspect the proposed collection and its destination. In this example, the export could contain a preview of the drawing, so it is not sent to the ordinary vendor support mailbox. Harbor Point and NorthStar arrange an authorized path or a different troubleshooting method.

Monitoring and recovery

Beacon receives the approved event feed. The feed has been reviewed for its normal fields, but the investigation procedure also addresses exceptional evidence. If Beacon requests a file sample, that request receives a separate handling review. Routine event access does not automatically authorize a larger evidence transfer.

The engineering workspace is backed up through the approved service. A failed job produces a neutral operational alert. Recovery, if needed, goes to the approved engineering destination rather than a general support share. The technician verifies access after restoration and records how temporary recovery material is handled.

Delivering and retaining the result

Harbor Point's authorized reviewer approves the final report and confirms the intended recipient. The engineer returns that exact version through the approved portal. The delivery record preserves the version reference and receipt information. A later correction follows the same review path rather than being emailed informally because the main project is nearly complete.

The customer retains the project material according to its applicable obligations and approved schedule. NorthStar maintains the agreed technical protections for retained and backup copies. Project closure triggers an access review and a check of temporary working locations. Ending active work does not establish that every copy has disappeared or that controlled information has been decontrolled.

This walkthrough produces more than a diagram. It gives the customer a narrative that the engineer, MSP, and monitoring provider can explain consistently. Any point they explain differently becomes a useful place to investigate before assessment preparation moves forward.

3.21 When information reaches an unapproved location

Now change one fact in the example. The engineer accidentally attaches a drawing screenshot to the ordinary help desk ticket. We need a response that limits further exposure while preserving enough evidence to understand what happened. The service desk should activate the agreed incident process and notify the designated customer contact.

Begin with facts: what was sent, when it was sent, which platform received it, and who or what may have accessed it. Consider automated notifications, integrations, previews, and backup behavior. Do not repeatedly download the attachment to investigate it on additional workstations. Use the approved evidence-handling process and restrict access through supported platform controls.

The customer and its designated incident personnel then determine the applicable reporting and preservation obligations. Where DFARS 252.204-7012 applies and its incident conditions are met, the clause specifies reporting within 72 hours of discovery and preservation of specified system images and relevant monitoring data for at least 90 days after the report. Those are conditional obligations, not a universal rule that every mistaken attachment in every business must be reported in the same way. [7]

Cleanup should follow an approved plan. Removing the visible ticket attachment may leave email copies or retained backups. Conversely, destroying every trace immediately may conflict with preservation needs. Record what the platform can remove, what remains under controlled retention, who authorized the actions, and what follow-up is required.

Finally, correct the workflow that permitted the mistake. A warning on a form may help, but the team should examine attachment permissions, routing, user guidance, and the availability of a practical protected support path. The incident is not fully addressed if the employee must choose between getting help and following the approved process.

3.22 Discovery tools and their limits

Automated discovery can help locate candidate information across large collections. It can search for markings, patterns, filenames, or content features. However, a search result is an indication for review, not an authoritative information determination. A search that returns no results is also limited by its coverage and detection method.

For example, a tool searching for a visible CUI banner may miss an unmarked derived spreadsheet. A text search may miss a scanned drawing without searchable text. A scanner may lack permission to inspect an archive. These are practical reasons to combine automated results with interviews, configuration review, and representative workflow tests.

Record what the discovery tool could access and what it excluded. Identify the locations reviewed, relevant permissions, file types, and known limitations. If the tool sends content to an external analysis service, review that flow before scanning. A discovery project should not create a new uncontrolled copy of the information it is trying to locate.

When a candidate is found, route it to the designated owner for review. Keep the result linked to the decision so the organization can distinguish a confirmed finding from a false positive or an unresolved question. Avoid teaching staff that a scanner's confidence score is equivalent to a contractual determination.

A practical measure of success is whether the team can explain its coverage and its remaining uncertainty. “No CUI found” is incomplete without knowing what was searched and how. “The reviewed locations contained these confirmed records; these

two archives remain unexamined” gives management a useful basis for the next action.

3.23 Turning discovery into evidence

Assessment preparation needs records that connect the described environment to its actual behavior. An information register explains decisions. A flow record explains movement. Configuration evidence and tests help show that the described restrictions exist. Interviews establish whether the responsible people understand and perform the process.

For Harbor Point, a focused evidence package might begin with IR-017 and the related contract clarification. It can then link the approved flow record, relevant configuration exports, a synthetic transfer test, a support procedure, and a sample of completed operational records. Keep each item tied to the proposition it supports.

A screenshot of a disabled download setting may support a configuration claim. It does not prove that every user, application, or device is subject to that setting. A test with one account may demonstrate one path but leave an administrator or guest path untested. State the coverage so the reviewer can understand the limits without having to infer them.

The evidence package itself needs controlled access. Do not distribute actual CUI widely merely to prove that the organization knows where it exists. Use neutral references or appropriately prepared examples when they satisfy the purpose. If actual content is necessary, agree on an authorized review method and preserve its handling restrictions.

Organize evidence around applicable requirements and assessment objectives during the later readiness work. This chapter's package is a discovery foundation, not a complete assessment submission and not proof that an entire requirement is met. Its value is that it makes subsequent control and scope analysis more accurate.

3.24 Common mistakes and how to correct them

A frequent mistake is treating a folder name as a determination. A directory called “CUI” can contain public documents, while a directory called “General” can contain controlled material. Correct the problem by examining representative content and its basis, then aligning the workflow and permissions with the resulting decision.

Another mistake is treating a customer statement as complete technical evidence. “We never download files” may describe policy rather than behavior. Check synchronization, temporary downloads, exports, and exceptional support actions. Preserve the customer's intent, but verify whether the system implements it.

A third mistake is assuming that encryption removes all further questions. Encryption can protect information under specified conditions, but it does not decide who may receive it, whether the offering is appropriate, or whether a backup restoration creates an unauthorized copy. Keep information status, authorization, architecture, and provider obligations as distinct parts of the review.

Teams also confuse deletion with decontrol. Deletion concerns a copy's disposition. Decontrol concerns removal of safeguarding or dissemination controls through the authorized process when appropriate. Removing a banner or completing the project does not establish that process has occurred. [8]

Finally, avoid documenting an ideal environment as though it already exists. If the approved design prohibits ticket attachments but the current system allows them, record the gap. Describe the current behavior, the intended change, and the verification needed. Assessment preparation becomes more reliable when documents expose unfinished work clearly.

3.25 Practice scenarios

Work through each scenario before reading the explanation. For each one, identify what is known, what remains uncertain, the immediate handling action, and the record you would retain. These exercises use fictional facts and do not assign status to any real customer information.

Scenario 1 The progress report

Harbor Point prepares a nonpublic monthly report solely to satisfy a Government contract deliverable. It contains ordinary schedule information and no identified controlled content. What is the most reasonable starting treatment?

Explanation: Under the stated assumptions, FCI is the appropriate starting analysis. Preserve the contract connection and content basis. Revisit the decision if controlled details are added. The report's title is less important than its purpose and contents.

Scenario 2 The invoice attachment

An employee says an invoice package is exempt because it is used for payment. The package includes a controlled inspection report. Can the whole package be treated as simple transactional information?

Explanation: No. Examine the components separately. The technical attachment does not lose its handling conditions because it accompanies a payment request. The organization can consider a workflow that separates routine payment data from the controlled supporting record.

Scenario 3 The unmarked spreadsheet

A spreadsheet from the prime reproduces measurements from a controlled drawing, but it has no banner. What should the engineer do?

Explanation: Use the agreed interim protective workflow and obtain clarification through the information owner. Record the source relationship and uncertainty. Do not post the spreadsheet to a general ticketing system to ask whether it is CUI.

Scenario 4 The public manual

A technician downloads a manual that the Government has lawfully released to the public without restrictions. Does storing it beside project records automatically make the manual CUI?

Explanation: No. Co-location alone does not create the designation. The repository may need protection because of its other contents, but the manual's information status requires its own basis. A later annotated version containing controlled project details may be different.

Scenario 5 The remote connection

A provider says its support method is outside scope because it uses remote access. The product permits file transfer, clipboard redirection, and local recording. Is the statement established?

Explanation: No. The actual configuration needs review, including any claimed VDI exception and the device's other functions. A product label does not demonstrate that the conditions of a specific scoping provision are met.

Scenario 6 The backup restore

A technician restores a controlled project folder into a general support share to check whether recovery worked. The backup itself used an approved service. What failed?

Explanation: The restoration introduced a destination that was not covered by the approved workflow. Restrict the new exposure and use the incident process as appropriate. Correct the recovery procedure so destination and access verification are part of success criteria.

Scenario 7 The AI summary

An engineer asks an unreviewed AI service to summarize a controlled report. The service says it does not use customer content for training. Is that enough to approve the transfer?

Explanation: No. The organization still needs to examine processing, storage, access, provider obligations, and the authorized use. The resulting summary may also contain controlled information. A training setting addresses only one aspect of the service.

Scenario 8 The security event

Beacon receives an event containing a username, timestamp, and sign-in result. An analyst later requests a full memory capture. Can the original feed approval cover the request automatically?

Explanation: No. The requested evidence has a different potential payload and handling path. Review the collection and transfer through the approved incident process. Do not assume all evidence fits the same arrangement because it supports security work.

Scenario 9 The closed project

The project has ended. A manager tells NorthStar to remove all CUI markings so the documents can move to ordinary archive storage. What is missing?

Explanation: Project closure is not evidence of authorized decontrol. The information owner must establish the applicable retention and handling decision. Until then, maintain the required protection and document any archive transfer through the approved process.

Scenario 10 The clean scan

A discovery scan returns no CUI matches. The scanner could not read encrypted archives and did not inspect scanned images. Can management conclude that the environment contains no CUI?

Explanation: No. Report the result within its actual coverage. Combine it with the contract review, interviews, and additional authorized examination of excluded locations. The unresolved coverage belongs in the findings register with an owner.

3.26 An MSP action checklist

Use this checklist after reading the chapter. Each completed item should point to a record or a demonstrated process. A checkmark without supporting facts is a progress note, not evidence of implementation.

1. Identify the customer information owner and the contracting contact who can obtain authoritative clarification.

2. Review the relevant contract instructions and record the versions used.

3. Identify representative FCI and CUI record types, including information created during performance.

4. Record the determination basis and unresolved questions without copying unnecessary sensitive content.

5. Trace receipt, use, collaboration, delivery, retention, and disposition for each important workflow.

6. Examine temporary files, support attachments, recordings, logs, integrations, backups, and restore destinations.

7. Review provider offerings and responsibilities for the information they actually handle.

8. Establish a practical protected support path and an escalation process for uncertain information.

9. Test the approved paths with synthetic data and document the limits of each test.

10. Reconcile the information register, flow records, configuration evidence, and current operational behavior.

11. Assign remediation owners for observed gaps and verify completed changes.

12. Set change triggers so new projects, recipients, tools, and service features prompt a fresh review.

3.27 Chapter review and preparation for scoping

We should now be able to explain what information the customer handles and how it moves through the work. That explanation should make sense to the contract owner, the engineer, the service desk, and the security provider. If one of them describes a different process, the difference deserves attention.

The distinction between FCI and CUI begins with the information and its governing context. The operational work then follows that information across formats and locations. An email, screenshot, derived report, backup, or diagnostic export can become significant because of what it contains and how it is used.

For NorthStar, the next useful step is to reconcile the information register with the technical environment. Every approved location should correspond to an understood service or asset. Every important flow should have an owner and a verified handling method. Unresolved questions should remain visible with a clear path to resolution.

This gives us a sound foundation for the later scoping chapter. We will have facts about the information, the work, and the supporting services. We can then apply the assessment rules to those facts and explain the resulting boundary with confidence appropriate to the evidence.

Official References

The following official sources support the definitions and requirements cited in this chapter. The operational examples, register designs, workshop method, and exercises are original teaching applications. The 2025 annual CFR edition is cited for the scoping provisions reviewed here; check the current rule and the applicable contract before using these examples to finalize an engagement.

[1] Federal Acquisition Regulation 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, paragraph (a). Clause dated November 2021; Acquisition.gov page reviewed September 19, 2026.

Open official source

[2] National Archives, About Controlled Unclassified Information. Program overview and definition of CUI.

Open official source

[3] National Archives, CUI Registry. Category descriptions and associated safeguarding or dissemination authorities.

Open official source

[4] National Archives, CUI Category Controlled Technical Information. Category description and listed authority.

Open official source

[5] Information Security Oversight Office, CUI What You Need to Know. Explanation of CUI Basic and CUI Specified.

Open official source

[6] National Archives, CUI Category Export Controlled. Distinction among the authorities listed for this category.

Open official source

[7] DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. May 2024 clause, paragraphs (a), (b)(2)(ii)(D), (c), and (e).

Open official source

[8] National Archives, CUI Frequently Asked Questions. Guidance on uncertain markings, contract instructions, reuse, and decontrol. Individual answers address different contexts; apply the relevant contract and agency direction.

Open official source

[9] 32 CFR 170.19, CMMC Scoping, 2025 annual edition, particularly paragraph (c) and Tables 3 and 4. The PDF begins with continuation text from the preceding section; section 170.19 begins later on its first page.

Open official source

CMMC for MSPs

From Readiness to Certification

Chapter 4

CMMC Level 1 and Level 2

By Dr. Charles Edwards

Teaching edition • September 2026

Chapter Purpose

This chapter explains CMMC Level 1 and Level 2 from the perspective of an MSP that must translate contract language into repeatable technical and operational services. The two levels are related, but they are not interchangeable. Level 1 protects Federal Contract Information through the fifteen basic safeguarding requirements in FAR 52.204-21. Level 2 protects Controlled Unclassified Information through the 110 security requirements in NIST SP 800-171 Revision 2 and a substantially more detailed assessment process.

The most important lesson is that Level 2 is not simply Level 1 with more tools. It changes how the organization defines scope, documents the system, evaluates external providers, collects evidence, manages deficiencies, and prepares people for assessment. An MSP that understands only the control titles will struggle. The provider must understand the desired security outcome, the assessment objectives, the customer responsibility, the evidence, and the normal operating process that keeps the requirement working after assessment day.

We will follow Harbor Point Engineering, NorthStar Managed Technology, and Beacon SOC through a practical decision: Harbor Point currently handles FCI under a Level 1 requirement but expects a new subcontract involving CUI. The case shows what must change when the company moves from a basic safeguarding environment to a Level 2 assessment scope.

Learning Objectives

- Explain the relationship among FAR 52.204-21, DFARS 252.204-7012, NIST SP 800-171 Revision 2, and CMMC.
- Describe the fifteen Level 1 requirements and their practical MSP implications.
- Explain the fourteen Level 2 requirement families and the role of NIST SP 800-171A assessment objectives.
- Distinguish Level 2 self-assessment from Level 2 C3PAO certification assessment.
- Describe scoring, conditional status, POA&M limitations, affirmation, and continuing compliance.
- Create a practical transition plan from Level 1 to Level 2.
- Identify evidence that demonstrates implementation rather than policy intent alone.

4.1 Begin with the Required CMMC Status

The customer does not select a level because it prefers a particular security package. The solicitation, contract, or flowed-down requirement identifies the CMMC status required for the information systems used in performance. The government requiring activity considers whether the work involves FCI or CUI and identifies the applicable status. At the subcontract level, the higher-tier contractor must flow the appropriate requirement based on the information and work being provided.

An MSP should ask for the actual contractual language. A customer statement such as “we need CMMC” is not specific enough to design the service. The provider needs to know whether the requirement is Level 1 Self, Level 2 Self, or Level 2 C3PAO; which systems will be used; what information will be processed; when the status is required; and which flowdown clauses and reporting duties apply.

The requirement applies to a defined information system and assessment scope. A company may operate one environment for ordinary corporate work and another for CUI. The MSP should avoid promising that the entire company is “Level 2 compliant” without identifying the system, boundary, and status being discussed.

Question	Why it matters
What information will the customer receive?	FCI and CUI lead to different security and assessment requirements.
What status appears in the solicitation or subcontract?	Level 2 Self and Level 2 C3PAO are different assessment paths.
Which systems will perform the work?	The status attaches to an assessment scope, not an abstract company label.
When must the status be current?	Architecture, remediation, evidence, and assessment scheduling require lead time.
What must flow to lower tiers?	Suppliers that handle FCI or CUI may require their own applicable status.

4.2 The Regulatory Chain in Plain Language

Level 1 and Level 2 are built from existing federal safeguarding obligations. CMMC adds a standardized method for assessing whether those obligations are implemented. Understanding the chain prevents the MSP from treating CMMC as a separate security framework disconnected from the customer’s contract.

Authority	Practical function	MSP implication
FAR 52.204-21	Establishes fifteen basic safeguards for covered contractor information systems containing FCI.	Provides the Level 1 security requirements.
DFARS 252.204-7012	Requires adequate security for covered defense information and includes cyber incident, preservation, and cloud provisions.	Connects CUI handling to NIST SP 800-171 and operational reporting duties.
NIST SP 800-171 Rev. 2	Defines 110 requirements for protecting CUI in nonfederal systems.	Provides the Level 2 security requirements incorporated by the current CMMC rule.
NIST SP 800-171A	Defines assessment objectives and examine, interview, and test methods.	Shows the depth of proof required for Level 2 implementation.
32 CFR Part 170	Establishes CMMC levels, assessment processes, scope, scoring, POA&M, affirmation, and ecosystem rules.	Determines how the security requirements are assessed for CMMC status.
DFARS 252.204-7021	Places current CMMC status, annual affirmation, reporting, and flowdown obligations into applicable contracts.	Makes status and continued compliance part of contract performance.

A common mistake is to read only one document. The MSP may implement NIST SP 800-171 controls but overlook DFARS incident reporting. It may read the CMMC rule but ignore the contract-specific level. It may rely on a policy crosswalk without examining NIST SP 800-171A objectives. The complete answer comes from the applicable contract and the incorporated authorities together.

4.3 Level 1 Overview

Level 1 focuses on FCI and uses the fifteen safeguarding requirements in FAR 52.204-21. The organization performs a self-assessment annually and records the required result through the government process. A senior affirming official must affirm continuing compliance annually. Level 1 does not allow a POA&M. Every applicable requirement must be MET to achieve the status.

Basic does not mean optional or informal. Small companies frequently rely on shared accounts, unmanaged personal devices, consumer routers, uncontrolled removable media, and undocumented support. These conditions can conflict with Level 1

requirements. The organization must be able to show that the safeguards work across every in-scope system that processes, stores, or transmits FCI.

Level 1 scope is comparatively direct: contractor information systems that process, store, or transmit FCI are in scope. Assets that do not handle FCI are outside Level 1 scope. The customer still needs a credible inventory and data-flow understanding to support that conclusion.

4.4 The Fifteen Level 1 Requirements

Safeguard area	Plain-language requirement	Typical MSP evidence
Access control	Limit system access to authorized users, processes acting for them, and authorized devices; limit permitted functions and transactions.	Account inventory, approvals, device controls, role configuration, and access-review records.
External systems	Verify and control connections to external systems and use of external systems.	Firewall rules, remote-access standards, approved service list, and connection reviews.
Public systems	Control information posted or processed on publicly accessible systems.	Website publishing approvals, content review, and removal process.
Identification	Identify users, devices, and processes.	Named accounts, asset identities, service-account inventory, and directory records.
Authentication	Authenticate or verify identities before granting access.	Password configuration, MFA where used, device certificates, and authentication logs.
Media sanitization	Sanitize or destroy media before disposal or reuse.	Media procedure, destruction certificates, tickets, and chain-of-custody records.
Physical access	Limit physical access and escort/monitor visitors.	Badge lists, visitor logs, escort procedure, and facility review.
Physical protection	Protect and monitor facilities and supporting infrastructure.	Door controls, alarm records, camera or monitoring evidence, and key inventory.
Communications protection	Monitor, control, and protect communications at external and key internal boundaries.	Firewall configuration, network diagram, approved flows, and rule reviews.
Network separation	Implement subnetworks for publicly	DMZ or hosted architecture,

Safeguard area	Plain-language requirement	Typical MSP evidence
	accessible components separated from internal networks.	segmentation rules, and validation tests.
Flaw remediation	Identify, report, and correct system flaws in a timely manner.	Patch reports, vulnerability tickets, exceptions, and verification.
Malicious code protection	Provide protection at appropriate system locations.	Endpoint coverage, policies, update health, detections, and response tickets.
Protection updates	Update malicious-code mechanisms when new releases are available.	Update policy, console status, exceptions, and remediation records.
System scanning	Perform periodic and real-time scans of files from external sources as appropriate.	Scan configuration, event logs, quarantine actions, and coverage reports.
Information system monitoring	Identify unauthorized use through monitoring.	Log sources, alert rules, review records, cases, and escalation evidence.

4.5 Implementing Level 1 as an Operating Service

An MSP should convert the fifteen safeguards into service workflows. Account control becomes an approved onboarding, change, review, and termination process. Media sanitization becomes a ticketed disposition workflow. Flaw remediation becomes a patch and vulnerability process with timelines, exceptions, and verification. Monitoring becomes defined log sources, alert handling, escalation, and retention.

The service should produce evidence automatically where possible. Named technician identities, access logs, patch reports, endpoint coverage, firewall reviews, and disposal records are stronger when they result from normal operations. Last-minute screenshots can supplement evidence, but they should not be the only proof that a safeguard operates throughout the year.

Level 1 also requires customer participation. The customer identifies who is authorized, controls public release decisions, secures facilities, reports personnel changes, and approves business exceptions. The MSP should place these dependencies in the service agreement and responsibility matrix rather than assuming the customer understands them.

4.6 Level 1 Self Assessment and Affirmation

A self-assessment is a formal evaluation, not a casual checklist. The organization should define the scope, identify responsible personnel, collect evidence, examine each requirement, document the result, correct deficiencies, and retain the assessment record. The assessor is the organization itself, but the standard for truthfulness does not change.

The affirming official is a senior representative who has responsibility and authority to affirm continuing compliance. That person needs more than a summary score. Management should receive the scope, material changes, open exceptions, evidence gaps, service-provider dependencies, and internal review results before affirming.

Because Level 1 permits no POA&M, an unmet safeguard must be corrected before the organization claims the required status. The MSP should identify this early. A sales deadline does not convert an unmet requirement into a met requirement.

4.7 Moving from FCI to CUI

When Harbor Point expects to receive CUI, its problem is not solved by changing the label from Level 1 to Level 2. The company must trace the CUI, define a Level 2 scope, categorize assets, document the system, implement 110 requirements, evaluate external providers, map assessment objectives, create evidence, and complete the required assessment pathway.

NorthStar begins with business workflow. Engineers receive technical data, collaborate, create derivatives, send deliverables, request support, and retain project records. Every action can introduce endpoints, cloud services, email, identity, network, printing, backup, monitoring, ticketing, and provider systems into the analysis. The MSP designs the technical boundary around this workflow rather than forcing a generic product bundle onto it.

The transition also changes governance. Harbor Point needs an SSP owner, an affirming official, requirement owners, evidence owners, change review, supplier oversight, incident coordination, and management review. NorthStar can support these functions but cannot replace the customer’s accountability.

4.8 Level 2 Overview

Level 2 protects CUI using all 110 requirements in NIST SP 800-171 Revision 2. The requirements are organized into fourteen families. Depending on the procurement, the

organization completes either a Level 2 self-assessment or a Level 2 certification assessment conducted by a C3PAO. Both pathways use the same 110 security requirements and the same underlying NIST SP 800-171A assessment objectives.

The difference is who performs the assessment and the status required by the procurement. An organization cannot substitute a self-assessment when the contract requires Level 2 C3PAO. The MSP should confirm the required status before creating the project schedule and should not promise that a readiness review is a certification assessment.

Level 2 path	Performed by	Status period	MSP preparation focus
Level 2 Self	The organization seeking assessment.	Final status is generally current for three years, with annual affirmation and no disqualifying change.	Defensible internal assessment, objective-level evidence, accurate SPRS submission, and continuing operations.
Level 2 C3PAO	An authorized or accredited C3PAO assessment team.	Final status is generally current for three years, with annual affirmation and no disqualifying change.	Assessment-ready scope, organized evidence, prepared personnel, demonstrations, secure provider participation, and remediation response.

4.9 The Fourteen Level 2 Families

Family	Operational meaning
Access Control	Authorized access, least privilege, remote access, wireless, mobile devices, and information flow.
Awareness and Training	Security awareness, role-based training, and recognition/reporting of threats.
Audit and Accountability	Log generation, review, correlation, protection, retention, and user accountability.
Configuration Management	Baselines, inventories, secure settings, change control, least functionality, and software restrictions.
Identification and Authentication	Unique identification, authentication, MFA, passwords, replay resistance, and credential management.
Incident Response	Preparation, detection, analysis, containment, recovery, reporting, testing, and coordination.

Family	Operational meaning
Maintenance	Controlled system maintenance, tools, personnel, remote maintenance, and sanitization.
Media Protection	Access, marking, storage, transport, sanitization, encryption, and removable media.
Personnel Security	Screening and protection during termination and transfer.
Physical Protection	Physical access authorization, monitoring, visitors, and alternate work sites.
Risk Assessment	Periodic risk assessment and vulnerability scanning with remediation.
Security Assessment	Control assessment, plans of action, monitoring, and SSP maintenance.
System and Communications Protection	Boundary protection, architecture, encryption, sessions, collaborative devices, and cryptographic keys.
System and Information Integrity	Flaw remediation, malicious code protection, monitoring, advisories, and unauthorized use detection.

The families are a way to organize requirements; they are not separate projects. Identity affects access control, audit, incident response, and remote maintenance. Configuration affects vulnerability management and system integrity. The SSP connects these relationships so the assessed system can be understood as one operating environment.

4.10 Understanding Assessment Objectives

NIST SP 800-171A breaks each requirement into one or more assessment objectives. Every applicable objective must be satisfied for the requirement to be MET. This is why reading only the requirement sentence is insufficient. One sentence may contain several facts that must be determined.

Assessment methods include examine, interview, and test. Examine reviews documents, configurations, records, and artifacts. Interview determines whether responsible people understand and perform the process. Test exercises or observes mechanisms and activities. Good preparation connects all three methods.

Requirement claim	Examine	Interview	Test
MFA protects privileged access.	Policy, scope, privileged account list, identity configuration, exceptions, and logs.	Identity administrator explains enrollment, coverage, exceptions, and review.	Demonstrate covered and blocked access paths.
Logs are reviewed.	Required sources, retention, alert logic, review records, cases, and approvals.	Analyst explains triage and escalation.	Trace a sample event through detection and response.
Accounts are terminated promptly.	Procedure, HR notification, closure ticket, directory record, and access review.	HR, manager, and service desk explain their roles.	Verify a selected former user has no remaining access.

4.11 Access Control

Access Control is broader than creating user accounts. The organization limits access to authorized users, processes, and devices; controls functions and transactions; applies least privilege; separates duties; manages remote and wireless access; controls mobile devices; and enforces approved information flows.

For the MSP, privileged administration is central. Technician access should use named identities, strong MFA, approved devices, restricted roles, monitored elevation, and prompt revocation. General-purpose access for every technician expands risk and makes evidence harder to defend.

Information flow control deserves equal attention. The MSP must understand how CUI moves between email, repositories, applications, printers, removable media, cloud services, backups, and support channels. A firewall alone cannot prevent a user from copying CUI into an unapproved SaaS platform.

4.12 Awareness and Training

Training must prepare people for the system they actually use. General annual awareness is not enough for personnel with specialized responsibilities. MSP technicians need instruction on remote access, ticket attachments, CUI recognition, secure exchange, escalation, prohibited tools, emergency access, and evidence handling.

Role-based training should occur before duties are performed and when the role or system changes. The organization should retain content, attendance, completion,

exceptions, and follow-up. Interviews should confirm that employees can apply the training rather than merely recall that they completed a course.

4.13 Audit and Accountability

Logging is an engineered capability. The organization decides which events are required, configures sources, synchronizes time, protects logs, collects them, reviews them, investigates anomalies, retains them, and confirms that sources remain healthy. Installing a SIEM satisfies none of these outcomes by itself.

NorthStar and Beacon SOC create a log-source inventory for Harbor Point. Each source has an owner, required events, retention, ingestion test, alert use, and failure response. Beacon documents cases and escalations. NorthStar corrects collection failures. Harbor Point approves risk and participates in incident decisions.

4.14 Configuration Management

Configuration Management establishes what the system should look like and controls change. The organization maintains inventories and baselines, uses secure settings, restricts unnecessary functions, controls software, documents changes, analyzes security impact, and verifies implementation.

An MSP often performs the technical change, but the customer may own approval. The process should record request, reason, affected assets, impact, authorization, implementation, test, rollback, evidence, and closure. Emergency changes require a defined retrospective review rather than disappearing into an ordinary ticket.

4.15 Identification and Authentication

Level 2 expects unique identification and authentication of users, processes, and devices, along with requirements for MFA, password management, replay resistance, obscured authentication feedback, and identifier handling. The goal is attributable and trustworthy access.

The MSP should inventory every access path: cloud portals, VPN, remote desktop, RMM, local administration, network devices, security consoles, service accounts, application programming interfaces, recovery accounts, and emergency access. MFA on the main portal does not compensate for a legacy protocol or local account that bypasses it.

4.16 Incident Response and DFARS Reporting

Incident Response includes preparation, detection, analysis, containment, recovery, reporting, testing, and lessons learned. DFARS 252.204-7012 adds contractual cyber incident reporting and evidence-preservation duties for covered defense information. The incident plan must connect operational response to those deadlines and authorities.

The MSP should define who may isolate a device, preserve an image, reset credentials, contact the customer, engage legal counsel, and submit the required report. Beacon SOC may detect the activity, NorthStar may contain it, and Harbor Point may hold the reporting obligation. A responsibility gap during the first hours can cause both security and contractual harm.

4.17 Maintenance and Media Protection

Maintenance requirements control tools, personnel, remote activity, and sanitization. A technician should not connect an unapproved diagnostic laptop or move files through a personal USB device. Remote maintenance must be authorized, strongly controlled, monitored, and terminated when complete.

Media Protection addresses digital and physical media across access, marking, storage, transport, sanitization, and encryption. Media includes more than removable drives. Printed drawings, backup media, exported logs, mobile devices, and retired storage require documented treatment. The MSP’s asset disposal process must preserve authorization and evidence.

4.18 Personnel and Physical Protection

Personnel Security requires screening and protection during termination and transfer. The customer controls employment decisions; the MSP often disables technical access. The process succeeds only when notification, authorization, timing, execution, verification, and evidence are coordinated.

Physical Protection covers facilities, equipment, visitors, access devices, monitoring, and alternate work sites. Cloud services do not eliminate local physical duties. Harbor Point must secure workstations, printed CUI, network equipment, and work areas. NorthStar must address where its authorized technicians work and what devices they use.

4.19 Risk and Security Assessment

Risk Assessment requires periodic risk evaluation and vulnerability scanning, including remediation. Security Assessment requires evaluation of controls, action plans, ongoing monitoring, and an accurate SSP. These activities turn security from a collection of tools into a managed program.

A vulnerability scanner is only one component. The MSP defines scope, verifies authenticated coverage, evaluates findings, assigns owners, tracks deadlines, documents exceptions, rescans, and reports trends. A risk decision belongs to authorized customer management, not to a technician who closes a finding because patching is inconvenient.

The SSP explains the system boundary, environment, requirements, implementation, relationships, and responsible parties. It should describe reality. A generic template that names nonexistent tools or processes makes assessment harder and may undermine confidence in the entire program.

4.20 System and Communications Protection

This family addresses architecture, boundaries, separation, encryption, sessions, collaborative devices, mobile code, Voice over IP, cryptographic keys, and related communication protections. The MSP should be able to show how traffic enters and leaves the environment and why each permitted path exists.

Encryption must be evaluated in context. The organization identifies where CUI is at rest and in transit, which cryptography protects it, how keys are managed, what exceptions exist, and whether the implementation meets applicable requirements. A product statement that “encryption is supported” does not show that it is enabled for every relevant path.

4.21 System and Information Integrity

System and Information Integrity addresses flaws, malicious code, security alerts, monitoring, spam protection, and detection of unauthorized use. MSP services frequently implement this family through patching, EDR, email security, SIEM, vulnerability management, and incident workflows.

Coverage and health matter as much as policy. The provider should reconcile expected assets with reporting assets, investigate unhealthy agents, confirm signature

and engine updates, monitor exclusions, review detections, and verify remediation. A console with missing systems is not complete protection.

4.22 A Detailed Level 1 Evidence Walkthrough

Because Level 1 is a self-assessment, some organizations assume a policy statement is enough. A defensible assessment connects each safeguard to the in-scope systems, the operating process, and evidence. The assessor should be able to select a user, device, facility, media item, network rule, or security event and trace how the safeguard applies.

For access control, Harbor Point begins with an authorized-user list approved by management. NorthStar compares the list with directory accounts, local accounts, application roles, remote-access groups, and administrative identities. Differences become tickets. The completed review includes the source reports, decisions, removed access, exceptions, reviewer, and date. This evidence shows a process rather than a single screenshot of one user.

For physical protection, Harbor Point identifies the office, server room, network closet, records area, and alternate work locations that support FCI processing. It documents who may enter, how access is granted and removed, how visitors are escorted, how keys or badges are controlled, and how unusual access is reviewed. NorthStar records where its technicians may work and which managed devices are approved for customer access.

For media sanitization, a retired laptop begins with an authorized disposal ticket. The ticket identifies the asset, storage media, information sensitivity, sanitization or destruction method, performer, verifier, date, and final disposition. If a disposal vendor is used, the organization retains the vendor record but does not rely on a certificate that cannot be connected to the specific asset.

For flaw remediation and malicious-code protection, NorthStar reconciles the asset inventory with patch and endpoint-security consoles. Missing agents, failed scans, overdue updates, and unsupported systems are treated as exceptions requiring action. Reports show not only successful devices but also failures, owners, corrective tickets, and verification. Management reviews the unresolved risk instead of receiving a misleading one-hundred-percent summary.

Level 1 evidence test	Weak answer	Stronger answer
Authorized access	“We use Microsoft 365.”	Approved user list reconciled to

Level 1 evidence test	Weak answer	Stronger answer
		accounts, roles, devices, and remote access with correction records.
Media disposal	“Our recycler wipes drives.”	Asset-linked authorization, sanitization method, performer, verifier, and disposition evidence.
Boundary protection	“We have a firewall.”	Current diagram, approved flows, rule set, review record, administrator access, and change tickets.
Flaw remediation	“Patches are automatic.”	Coverage, deployment rings, failures, exceptions, remediation, restart status, and verification.
Monitoring	“EDR sends alerts.”	Expected assets, healthy coverage, detections, analyst review, escalation, response, and retained cases.

4.23 The Level 2 Assessment Lifecycle

A Level 2 assessment should be treated as a lifecycle rather than a meeting with assessors. The lifecycle begins when the organization confirms the requirement and continues through scope definition, implementation, internal assessment, evidence maturation, the formal assessment, remediation, affirmation, and continuous monitoring.

During planning, Harbor Point identifies the required status, target date, CAGE information, assessment scope, affirming official, internal assessment lead, technical owners, provider contacts, and decision authority. NorthStar identifies the services and personnel it will contribute. Beacon identifies the evidence and demonstrations associated with monitoring and incident detection.

During implementation, the parties write implementation statements at the assessment-objective level. Each statement names the assets, configuration, process, responsible role, frequency, and evidence. A statement such as “MFA is enabled” becomes a description of which privileged and nonprivileged access paths require MFA, how enrollment and exceptions work, how coverage is reviewed, and which logs demonstrate operation.

During internal assessment, the team uses examine, interview, and test. It samples actual records instead of accepting process-owner assurances. When the result is NOT MET, the team identifies the precise objective, affected assets, root cause, corrective action, owner, validation method, and evidence-maturation period. Correcting a setting on Friday does not show that the operating process has worked for months.

During the formal assessment, the organization controls the evidence flow. Requests are logged, artifacts are reviewed for customer separation and sensitive content, interviews use personnel who perform the work, and demonstrations occur in the approved environment. The assessment coordinator tracks open questions without coaching employees to provide answers that differ from reality.

After the assessment, conditional items receive immediate executive attention. Final findings are incorporated into risk and improvement work. The organization preserves the assessment record, confirms annual affirmation responsibilities, and evaluates future changes against the assessed state.

4.24 Level 2 Self Assessment Versus C3PAO Assessment

Dimension	Level 2 Self	Level 2 C3PAO
Assessor	Qualified personnel acting for the organization.	Authorized or accredited C3PAO assessment team.
Independence	The organization must manage bias and verify its own conclusions.	External team evaluates the organization under the CMMC assessment process.
Preparation standard	Objective-level evidence and honest examine, interview, and test remain necessary.	The same requirements and objectives must be demonstrated to external assessors.
Result handling	Result is entered through the applicable government process.	Assessment result is processed through the CMMC ecosystem and government systems.
MSP participation	MSP supplies evidence, interviews, and demonstrations to the customer's internal team.	MSP participates under customer coordination and secure assessor-request procedures.
Procurement use	Valid only when the procurement requires Level 2 Self.	Required when the procurement specifies Level 2 C3PAO.

The self-assessment path should not be treated as an easier technical standard. The 110 requirements do not change. The organization must still satisfy the applicable objectives and affirm compliance. A weak self-assessment can create serious contractual and legal risk because the organization is making a representation about its implementation.

The C3PAO path adds external coordination, scheduling, evidence exchange, assessor interviews, demonstrations, and formal findings. The MSP should assign one assessment liaison and backups rather than allowing every technician to answer requests independently. The liaison confirms scope, protects unrelated customer information, and ensures that the correct subject-matter expert responds.

4.25 SPRS Records and the Affirmation Workflow

The Supplier Performance Risk System is used for applicable assessment results and affirmations. The organization should decide who is authorized to enter information, who validates the score and scope, which identifiers apply, and how submission evidence is retained. The MSP may support the technical assessment, but the customer should control its official representation unless a documented authority says otherwise.

Before submission, management should review the assessment type, date, scope, score, CAGE information, system identifiers, conditional items, and supporting record. Errors in scope or identity can cause confusion during contract verification. The submitted result should match the evidence package and management briefing.

Annual affirmation requires a repeatable governance process. Harbor Point schedules a quarterly compliance review and a formal pre-affirmation review. NorthStar provides access, vulnerability, configuration, patch, backup, logging, and provider-status reports. Beacon provides monitoring coverage, case metrics, and material incident information. Harbor Point reviews personnel, physical, contractual, training, and information-handling changes.

The affirming official receives a concise but complete decision package: current assessment status, scope, changes since assessment, control-health indicators, unresolved deficiencies, provider changes, incidents, evidence gaps, and management actions. If the assessed condition is no longer accurate, the organization addresses the problem rather than treating affirmation as an administrative renewal.

4.26 Mapping MSP Services to Level 2 Evidence

MSP service	Requirements commonly supported	Evidence package
Identity administration	Access Control; Identification and Authentication; Personnel Security.	Approved requests, role reports, MFA configuration, authentication logs, access reviews, termination tickets.
RMM and endpoint management	Configuration Management; System and Information Integrity; Maintenance.	Inventory, baselines, script approvals, patch status, agent health, technician activity, change records.
SIEM and SOC	Audit and Accountability; Incident Response; System and Information Integrity.	Log-source inventory, ingestion health, retention, alerts, cases, escalations, exercises, analyst interviews.
Vulnerability management	Risk Assessment; System and Information Integrity.	Authenticated coverage, findings, prioritization, tickets, exceptions, rescan confirmation, trend review.
Backup and recovery	Media Protection; System and Communications Protection; contingency-related operational support.	Configuration, encryption, access, jobs, failures, restore tests, retention, provider boundary.
Network management	Access Control; Configuration Management; System and Communications Protection.	Diagrams, rule sets, change approvals, administrative access, firmware status, rule reviews, segmentation tests.
PSA and documentation	Security Assessment; multiple operational requirements.	Controlled service descriptions, tickets, approvals, evidence index, permissions, retention, and customer separation.

The table does not assign an entire family to the MSP. It shows where provider services commonly contribute. The customer may retain approval, policy, risk, physical, personnel, and contractual responsibilities. Each assessment objective should be mapped to the exact contribution rather than using a broad statement that the MSP “handles security.”

Evidence should be collected at a planned cadence. Monthly coverage reports, quarterly access reviews, annual training, event-driven termination records, and change-based configuration evidence have different rhythms. The evidence index should identify the source, owner, frequency, retention, review, and secure location.

4.27 Conducting a Mock Assessment

A mock assessment should resemble the real evaluation closely enough to reveal operational weaknesses. It begins with a frozen scope package: SSP, diagrams, inventories, asset categories, provider list, and CRM. If the team changes the boundary every time evidence is difficult, the exercise cannot test readiness.

23. Select a representative sample of users, privileged accounts, endpoints, servers, network devices, applications, locations, changes, incidents, vulnerabilities, and terminations.
24. Examine policies, procedures, configurations, reports, tickets, logs, approvals, and retained evidence for the selected period.
25. Interview the people who perform the work, including customer staff, MSP technicians, service managers, security analysts, and system owners.
26. Test technical mechanisms and workflows, including access denial, MFA, log generation, alert escalation, session termination, secure transfer, restoration, and segmentation.
27. Record MET or NOT MET at the assessment-objective level with a clear evidence citation and rationale.
28. Identify systemic causes. A missing ticket may reflect one error, or it may reveal that the process never requires evidence.
29. Remediate the control, repeat the test, and allow sufficient operating evidence to develop before scheduling the formal assessment.

The mock team should include someone independent of the implementation work when practical. An engineer who built the control may unconsciously fill gaps with knowledge that is not present in the documentation or evidence. A fresh reviewer tests whether another qualified person can understand and verify the implementation.

4.28 Level 2 Scoring

Level 2 uses a weighted scoring methodology based on the 110 NIST SP 800-171 requirements. The maximum score is 110. When a requirement is NOT MET, points are subtracted according to its assigned value. Some deficiencies carry greater weight because they affect fundamental protections such as access, authentication, incident reporting, or encryption.

A score is not permission to ignore the underlying finding. The score supports assessment status and POA&M eligibility, but each NOT MET requirement remains a

real security deficiency. Management should review the affected objective, assets, risk, evidence, corrective action, owner, resources, and completion date.

The MSP should never manipulate the score by redefining scope after discovering weak controls. Scope must follow the official requirements and actual environment. Architectural scope reduction is valuable when designed honestly before assessment, not when used to hide connected systems.

4.29 Conditional Status and POA M

CMMC permits a conditional Level 2 status only under defined conditions. The organization must meet the minimum score, and certain requirements are ineligible for a POA&M. Eligible unmet items must be documented and corrected within the permitted 180-day period, followed by the appropriate closeout assessment.

A POA&M identifies the deficiency, corrective tasks, resources, milestones, owner, and completion dates. It is not evidence that the requirement is met. The assessment result remains NOT MET until the objective is successfully closed. The MSP should treat the closeout deadline as a managed project with executive visibility.

Foundational requirements should be resolved before the assessment whenever possible. Entering an assessment with known deficiencies can create schedule, contract, and reputation risk. A readiness review should identify gaps early enough for testing and evidence to develop after remediation.

4.30 Affirmation and Continuing Compliance

Level 2 status is not a three-year vacation from compliance. The affirming official must affirm continuing compliance annually. Material changes in systems, providers, locations, architecture, or implementation may affect the accuracy of the assessed state. The organization needs a process for evaluating change against scope and requirements.

NorthStar adds a CMMC impact field to change records. Changes involving identity, remote access, cloud services, backup, logging, CUI repositories, encryption, or external providers require security review. Harbor Point receives a periodic compliance report showing scope changes, exceptions, overdue actions, evidence health, and supplier status.

4.31 Level 1 and Level 2 Comparison

Dimension	Level 1	Level 2
Protected information	FCI	CUI
Security requirements	15 FAR 52.204-21 safeguards	110 NIST SP 800-171 Rev. 2 requirements
Assessment	Annual self-assessment	Self-assessment or C3PAO assessment as specified
Assessment depth	Applicable Level 1 objectives	NIST SP 800-171A objectives using examine, interview, and test
Scope	Systems that process, store, or transmit FCI	CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, providers, and connections as applicable
Documentation	Evidence sufficient to support the self-assessment	SSP, inventory, diagrams, policies, procedures, CRM, objective-level evidence, and operational records
POA&M	Not permitted	Limited conditional pathway for eligible requirements
Affirmation	Annual	Annual
MSP role	Operate basic safeguards and produce evidence	Support architecture, scope, 110 requirements, providers, evidence, assessment, and continuous compliance

4.32 Harbor Point Transition Case Study

Harbor Point currently uses ordinary corporate email, unmanaged home computers for occasional work, a shared network drive, and NorthStar's standard commercial support stack. This may already create Level 1 weaknesses. Before accepting the CUI subcontract, the company decides to build a defined enclave rather than place the entire enterprise in Level 2 scope.

NorthStar maps the proposed workflow. CUI enters through an approved portal, is processed on managed engineering workstations, is stored in a restricted repository, and is transmitted back through the approved channel. The design prohibits CUI in ordinary email and the PSA. Diagnostic files move through a controlled exchange.

Printing is restricted and documented. Backup uses an evaluated offering. Beacon SOC monitors the enclave.

The team categorizes assets. Engineering workstations and the repository are CUI Assets. Identity, firewall, EDR, SIEM, vulnerability, backup-management, and privileged access services are evaluated for their role and data. Corporate systems that can reach the enclave are not automatically out of scope. The team designs and tests separation, then documents risk-managed and out-of-scope decisions.

Harbor Point and NorthStar map every NIST SP 800-171A objective. Each objective receives an owner, implementation statement, evidence source, test method, and status. When evidence is missing, they determine whether the control is absent or merely undocumented. They correct the control first and allow normal operations to produce reliable evidence.

A mock assessment finds five major problems: two former technicians retain portal roles; several endpoints are missing authenticated vulnerability coverage; a firewall change lacks approval; the incident plan does not connect Beacon’s alert to DFARS reporting; and the backup service description does not identify the exact cloud offering. The team treats these as operating failures, not documentation edits.

After remediation, NorthStar demonstrates access, logging, vulnerability, backup, and change processes. Beacon traces a security event from ingestion through escalation. Harbor Point personnel explain information handling, approvals, incident decisions, and physical protection. The result is an environment that can be operated and explained, not simply a collection of compliant-looking documents.

4.33 Common Mistakes

Assuming Level 1 means no documentation

A self-assessment still requires a defined scope, evidence, accurate results, and management affirmation.

Treating Level 2 as a product bundle

Tools support requirements; they do not create governance, responsibility, evidence, or truthful implementation.

Using NIST SP 800-171 Revision 3 for the current assessment without contractual direction

The current CMMC rule incorporates Revision 2; applicability must follow the governing requirement.

Stopping at requirement titles

Level 2 is evaluated through detailed NIST SP 800-171A objectives.

Ignoring external-provider evidence

A customer cannot prove provider-operated controls with a contract and invoice alone.

Planning to fix everything on a POA&M

Eligibility is limited, the minimum score applies, and closeout is time-bound.

Preparing people to recite answers

Personnel should understand and perform the real process, not memorize an assessment script.

Treating certification as permanent

Annual affirmation and change management require continuing compliance.

4.34 Practical Transition Roadmap

Phase	Primary work	Deliverable
1 Contract and information	Confirm clauses, status, CUI, flowdown, dates, and stakeholders.	Contract requirements summary and information-flow record.
2 Scope and architecture	Design boundary; inventory and categorize assets, providers, users, and locations.	Scope statement, diagrams, inventories, and architecture decision.
3 Requirements and responsibility	Map 110 requirements and objectives to customer, MSP, and providers.	CRM, implementation matrix, and SSP structure.
4 Remediation	Correct technical, procedural, contractual, and personnel gaps.	Verified remediation tickets and updated baselines.
5 Evidence and rehearsal	Collect operational evidence; conduct interviews, demonstrations, and mock assessment.	Objective-level evidence index and readiness report.

Phase	Primary work	Deliverable
6 Assessment and sustainment	Complete required assessment, close eligible POA&M items, affirm, and monitor change.	Current status, affirmation record, continuous-compliance plan.

4.35 MSP Action Checklist

- Obtain the exact Level 1 or Level 2 status required by the solicitation, contract, or flowdown.
- Confirm where FCI or CUI enters, moves, is stored, is backed up, and leaves the environment.
- Define the assessment scope before selecting the final toolset.
- Map provider services to CUI, SPD, requirements, assessment objectives, and evidence.
- Create customer-specific inventories, diagrams, service descriptions, and a responsibility matrix.
- Evaluate every privileged access path, including emergency, local, service, and API access.
- Establish objective-level evidence owners, retention, review, and secure delivery.
- Perform an internal assessment using examine, interview, and test methods.
- Correct foundational deficiencies before scheduling the assessment.
- Brief the affirming official on scope, status, changes, exceptions, and evidence.
- Operate recurring reviews so the assessed condition remains true after certification.

4.36 Practice Scenarios

Scenario 1

The Level 1 customer uses a shared accounting computer that receives FCI by email.

Discussion: Identify the in-scope system and assess account, device, malware, flaw-remediation, monitoring, and physical safeguards.

Scenario 2

A Level 2 customer enables MFA in its cloud tenant but permits local admin passwords on enclave laptops.

Discussion: Map every privileged path and determine whether authentication objectives are fully satisfied.

Scenario 3

The SIEM has ninety days of logs, but the SSP says one year.

Discussion: Reconcile documentation, contractual needs, operational configuration, and assessment evidence.

Scenario 4

A vulnerability scan excludes a legacy server because credentials fail.

Discussion: Treat the server as uncovered, correct authentication or document a compliant alternative, and verify with rescan.

Scenario 5

A technician places a CUI screenshot in the PSA.

Discussion: Contain the information, follow incident and improper-transfer procedures, evaluate provider scope, and redesign the workflow.

Scenario 6

Harbor Point scores above the conditional threshold but has an ineligible requirement unmet.

Discussion: Conditional status is not available until the ineligible requirement is fully met.

Scenario 7

The backup vendor changes the service region.

Discussion: Perform provider and scope impact review before accepting the material change.

Scenario 8

A former employee still appears in an application role report.

Discussion: Investigate the termination process across all accounts, revoke access, verify, and retain corrective evidence.

Scenario 9

The customer passes assessment but replaces its identity platform six months later.

Discussion: Evaluate material change, requirements, scope, evidence, testing, and affirmation impact.

Scenario 10

The MSP has excellent policies but technicians routinely bypass change approval.

Discussion: The requirement is not operating as documented; correct the workflow, accountability, and evidence.

4.37 Chapter Review

CMMC Level 1 and Level 2 protect different information and demand different depths of implementation and assessment. Level 1 applies fifteen FAR safeguards to systems handling FCI and requires a complete annual self-assessment and annual affirmation. Level 2 applies 110 NIST SP 800-171 Revision 2 requirements to the defined CUI environment and uses detailed NIST SP 800-171A objectives.

For the MSP, success depends on translating requirements into stable services: named access, controlled change, healthy security coverage, documented response, reliable evidence, and clear customer/provider responsibilities. Level 2 is not achieved through documentation alone, and certification is not maintained through inattention. The system must continue to operate as assessed.

The next chapter will use this foundation to define the CMMC assessment scope in detail, including asset categories, enclaves, segmentation, external providers, remote administration, and defensible boundary decisions.

Review Questions

1. What information does Level 1 protect, and which requirements apply?

2. Why is Level 1 more than an informal checklist?

3. What four authorities connect the contract to Level 2 implementation and assessment?

4. Why must an MSP examine NIST SP 800-171A objectives?

5. What is the difference between Level 2 Self and Level 2 C3PAO?

6. How do examine, interview, and test support one another?

7. Why does MFA require an access-path inventory?

8. What makes vulnerability scanning an operational process rather than a tool?

9. Why is a POA&M not evidence that a requirement is met?

10. What must the affirming official understand before annual affirmation?

11. How can a material provider change affect continuing compliance?

12. Which Level 2 family presents the greatest challenge for a typical MSP customer, and why?

Key Terms

Term	Meaning
Affirming Official	Senior representative responsible for ensuring and affirming continuing compliance.
Assessment objective	Determination statement used to evaluate whether a requirement is successfully implemented.
C3PAO	Authorized or accredited organization conducting Level 2 certification assessments.
Conditional status	Time-limited status available only when scoring and POA&M conditions are satisfied.
FCI	Nonpublic federal contract information protected at Level 1.
CUI	Controlled Unclassified Information protected at Level 2 or Level 3.
NIST SP 800-171A	Assessment procedures and objectives for NIST SP 800-171 requirements.
POA&M	Plan identifying eligible deficiencies, tasks, resources, milestones, and dates; not a substitute for implementation.
SPRS	Supplier Performance Risk System used for applicable assessment and affirmation records.
SSP	System Security Plan describing the system and implementation of requirements.

Official References

- Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. Current through September 2026. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
- Acquisition.gov. FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. https://www.acquisition.gov/far/52.204-21
- Acquisition.gov. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. https://www.acquisition.gov/dfars/252.204-7012
- Acquisition.gov. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements. https://www.acquisition.gov/dfars/252.204-7021
- National Institute of Standards and Technology. SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
- National Institute of Standards and Technology. SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information. https://csrc.nist.gov/pubs/sp/800/171/a/final

Regulatory note: Requirements and acquisition rules may change. Confirm the current contract, eCFR, DFARS, official DoD guidance, and incorporated publications before making compliance decisions.

CMMC for MSPs

From Readiness to Certification

Chapter 5

Defining the CMMC Assessment Scope

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and regulatory context — 3

5.1–5.5 Business workflows and information flows — 4

5.6–5.14 Levels and asset classification — 9

5.15–5.19 Architecture, administration, and MSP tools — 18

5.20–5.25 Providers, cloud, and operational flows — 23

5.26–5.30 Scope documentation and verification — 28

5.31 Harbor Point scoping case study — 34

5.32–5.34 Scope changes and common mistakes — 37

5.35–5.37 Scenarios, workshop, and chapter review — 40

Official references — 47

Chapter Purpose

Before an MSP can prepare a customer for a CMMC assessment, it must establish what is being assessed. That sounds like a simple inventory exercise. In practice, it is one of the most consequential decisions in the entire engagement. A missing backup service, an overlooked remote administration path, or an incorrect assumption about an employee's laptop can change the environment that must be explained, protected, and assessed.

This chapter teaches a method for defining and maintaining that environment. We will begin with the work the customer performs, follow the information through the work, identify the assets and services involved, and apply the appropriate scoping categories. We will then connect those decisions to the system security plan, diagrams, inventories, responsibility records, and evidence. The result should be a scope that the customer can operate and that another qualified person can understand.

The main conclusion is straightforward: a scope statement must describe the real environment. It cannot be built from the customer's preferred assessment price or the MSP's standard product package. A smaller environment may be practical and defensible, but only when its architecture, information handling, administration, and supporting services sustain the proposed boundary.

We continue with Harbor Point Engineering, its MSP NorthStar Managed Technology, and its monitoring provider Beacon SOC. These organizations and all examples, asset identifiers, staffing arrangements, costs, and project events in this chapter are fictional teaching material. Their purpose is to make the decisions understandable without suggesting that one design fits every customer.

Learning Objectives

- Explain the difference between an organizational boundary, a network boundary, and a CMMC assessment scope.
- Trace FCI, CUI, and security protection data through business and support workflows.
- Apply the Level 2 asset categories and explain their different assessment treatment.
- Analyze external providers, remote administration, backup, cloud services, and shared MSP tools.
- Develop a coherent scope statement, inventory, data-flow record, diagram set, and responsibility matrix.

- Verify proposed exclusions through documented reasoning and appropriate technical tests.
- Maintain the scope when users, applications, locations, providers, and business requirements change.

Regulatory context for this edition

This chapter explains the scoping framework in 32 CFR 170.19 and its associated definitions in 32 CFR 170.4. It concentrates on Level 2, while explaining the important differences at Levels 1 and 3. The specific assessment required for a customer must follow its applicable contractual requirements and current official direction. [R1, R2]

The official CMMC program notice reports that the planned Phase II rollout was suspended on July 13, 2026, and that Phase I self-assessment requirements remain in place. Accordingly, this chapter does not assume that the previously announced Phase II date is an automatic certification deadline for every customer. Confirm current implementation direction and the customer's actual solicitation, contract, and flowdown before scheduling an assessment or promising a delivery date. The scoping methods remain relevant to protecting the information and preparing a supportable assessment. [R7]

The regulatory explanations identify the governing sources. The sample workflows, review frequencies, record formats, and tests are practical teaching examples unless expressly identified as requirements. They should be adapted to the customer's environment and evaluated against the applicable rules.

5.1 Start with the work the customer performs

An MSP often receives an opening request such as, "We need a CMMC environment for twelve people." Before discussing twelve laptops, ask what those people do. Are they reading contract schedules, designing components, analyzing test results, reviewing drawings, or supporting a production process? Where does the information originate, and what must the customer return? Those answers give meaning to the technology inventory.

At Harbor Point, the initial request concerns an engineering subcontract. The engineers receive design material, modify drawings, exchange questions with the prime contractor, and return deliverables. The work may involve applications, temporary files, review comments, printed output, backup copies, and technical

support. A scope that includes only the final drawing folder would miss much of the actual workflow.

Begin the discovery meeting with a business owner and at least one person who performs the work. The business owner understands the contract and the intended process. The employee can explain the ordinary exceptions: a portal that times out, an application that creates local copies, or a reviewer who sends corrections by email. Both perspectives are necessary. A process that works only in the manager's description will not define a reliable boundary.

NorthStar records the work in plain language before turning it into a diagram. For example: an authorized engineer receives a drawing through the approved exchange, opens it in the design application, saves the revision in the controlled repository, and returns it through the approved exchange. Each verb becomes a discovery question. Receive may involve email notifications; open may create a local cache; save may trigger synchronization; return may include a support or review service.

The initial deliverable is a short business workflow description with named owners and unresolved questions. It is not yet a final scope. Its value is that it prevents the project from choosing a technology boundary before understanding the activity that boundary must support.

5.2 Distinguish the boundaries being discussed

An organizational boundary identifies the business entity, personnel, locations, and responsibilities involved. A network boundary describes connectivity and traffic control. An assessment scope identifies the assets to be assessed under the applicable CMMC rules. These boundaries interact, but they are not interchangeable. An asset can sit outside the customer's building and still matter to the assessment.

Consider a cloud identity service that controls access to Harbor Point's engineering repository. It may be operated outside Harbor Point's physical facilities, yet it provides a security function for the assessed environment. Conversely, a device physically present in the office may be outside the Level 2 scope if it meets the out-of-scope criteria. Physical location alone does not settle either decision.

The rule requires the assessment scope to be specified before assessment. That scope must be derived from the relevant asset categories and their treatment, rather than merely from a colored rectangle around the engineering subnet. The diagram is a representation of the decision; it is not the authority that creates the decision. [R1]

A useful way to organize the first discussion

Ask three questions in order. First, what organization and contractual work are involved? Second, where does the relevant information go, and what protects it? Third, which assets and services fall within the applicable scoping treatment? This sequence keeps business context, technical reality, and assessment rules connected.

NorthStar should also distinguish an assessment scope from its own service scope. The MSP agreement may cover endpoint management and network support but exclude personnel screening, physical access, or contract administration. Those exclusions from the MSP's services do not remove the customer's corresponding assessment responsibilities. Record who performs the work that the MSP does not provide.

Boundary	Main question	Example
Organization	Who owns the work and decisions?	Harbor Point and its authorized staff
Network	What can communicate through which paths?	Engineering segment and approved gateways
Assessment	What receives the applicable CMMC treatment?	CUI assets and relevant supporting assets
MSP service	What has NorthStar agreed to deliver?	Identity administration and endpoint support

5.3 Confirm the information before classifying the assets

FCI, CUI, and ordinary commercial information should not be treated as interchangeable labels. The nature of the information affects the safeguarding and assessment analysis. A customer may use the word sensitive to mean pricing information, personal information, a trade secret, FCI, or CUI. Ask what the term means in the particular workflow rather than translating every use of sensitive into CUI.

The CUI Registry identifies categories and associated authorities. The contract and authorized information owner help establish what the customer receives or generates and which requirements apply. An MSP should not independently designate every drawing as CUI or assume that an unmarked item can never be CUI. When the source

and contractual direction are unclear, record the question and obtain clarification through the appropriate channel. [R3]

For Harbor Point, the discovery record identifies the source of the engineering material, the relevant contractual direction, the information category when established, the expected recipients, and the approved means of exchange. NorthStar does not need to collect real controlled drawings into its general project workspace merely to ask these questions. A description, appropriately handled sample, or authorized demonstration may provide the necessary understanding.

Information generated during performance deserves attention. An engineer may create a revised drawing, analysis, test result, or annotation derived from the supplied material. The workflow review must consider whether the resulting information retains applicable controls. Changing the file name or converting a drawing to a PDF does not by itself settle its handling requirements.

Resolve uncertainty explicitly

Use an unresolved-information record with an owner, question, interim handling direction, and decision date. For example, Harbor Point may need the prime contractor to clarify the status of a particular test dataset. The customer decides how to protect and restrict that dataset while obtaining the answer. NorthStar records the resulting scope assumptions and revises them when clarification arrives.

Do not hide the uncertainty in a final diagram. If the classification affects whether an application must be included, the architecture decision is provisional until the underlying question is resolved. A transparent assumption is easier to manage than a confident but unsupported exclusion.

5.4 Follow information through its full lifecycle

A data-flow review should start before the first application screen and continue after the last deliverable is sent. Identify how information is received, processed, stored, shared, retained, backed up, restored, archived, and disposed of. Include both normal work and the supporting actions required to keep that work functioning.

Suppose an engineer downloads a file from a customer portal. The browser may write it to a downloads folder before the engineer moves it to the repository. The design application may produce an autosave file. A synchronization client may create another copy. A backup process may retain a deleted version. The data-flow

description should account for these locations rather than assuming that the intended final folder is the only storage location.

Include failed and interrupted operations. A transfer that fails halfway may leave a temporary file. A crashed application may produce a diagnostic package. A restore exercise may place a recovered copy on a test system. These are ordinary operational events, and the scoping analysis should explain how the organization handles them.

Write one record for each meaningful movement

NorthStar gives a flow an identifier, such as HP-FLOW-03. The record identifies the source, destination, information involved, initiating person or process, transfer method, purpose, relevant protection, and supporting evidence. An owner confirms whether the flow is approved and whether the diagram represents it correctly.

For a backup flow, the source may be the engineering repository and the destination the selected backup offering. The record should distinguish the protected payload from backup configuration and job records. Those different types of information may lead to different asset and provider questions. A line labeled backup on the network diagram is useful only when the team understands what that line represents.

Flow record field	Teaching example
Identifier	HP-FLOW-03
Business purpose	Recover engineering project files
Source and destination	Controlled repository to approved backup service
Information	Project payload plus separately analyzed job metadata
Initiator	Scheduled backup process
Owner	Harbor Point system owner with NorthStar support
Evidence	Service configuration and a controlled restore record

5.5 Find copies that ordinary inventories miss

A hardware inventory can tell the MSP that a laptop exists without showing where its applications place information. Supplement inventory discovery with application walkthroughs and configuration review. Ask about download folders, cached attachments, thumbnails, indexing, print spools, collaboration histories, offline files, browser extensions, and application export functions where relevant.

At Harbor Point, the design application writes a recovery copy to a user profile. The engineer does not think of that folder as project storage because the application manages it automatically. NorthStar verifies the behavior in an authorized test and records the resulting storage location. The laptop's CUI role is not avoided simply because the employee never manually saved the recovery copy.

Support activity can create a second group of hidden copies. A screenshot may enter a ticket. A remote session may be recorded. A diagnostic archive may contain fragments of documents or memory. A technician may copy a file to compare versions. Review the product's settings and the actual support workflow to determine which of these activities occur.

Investigate without spreading the information

Discovery should not create uncontrolled copies of the material being investigated. NorthStar uses approved access, customer-specific work locations, and authorized test data where practical. If a content search is needed, the customer approves its scope, method, access, and handling of results. Search results themselves may contain sensitive content and require protection.

An unexpected copy requires a response, not a quiet edit to the inventory. Establish what happened, protect the material, notify the appropriate customer personnel, follow the applicable incident or improper-transfer process, and correct the workflow. Then revisit the scope decision. Removing the visible file may not address retained versions, backups, indexes, or the process that created it.

5.6 Apply the Level 1 scope on its own terms

Level 1 scope begins with organizational information systems that process, store, or transmit FCI. The rule also contains specific treatment for specialized assets and a defined VDI-client condition. Do not take the Level 2 asset-category table and apply it unchanged to Level 1. The two levels have different scoping structures. [R1]

For an ordinary FCI workflow, NorthStar identifies the systems used to receive, prepare, store, and exchange the information, along with the relevant people, facilities, and external services. A small contractor may discover that FCI appears in an office mailbox, a shared drive, and an employee laptop. Restricting the assessment to the shared drive would not describe the workflow.

The Level 1 rule excludes specialized assets from its assessment scope and does not require documentation of out-of-scope assets. It also describes an out-of-scope VDI endpoint condition where no FCI processing, storage, or transmission is allowed beyond the specified keyboard, video, and mouse interaction. These are particular regulatory treatments, not a general permission to ignore difficult equipment or every device running a remote desktop client. [R1]

An MSP may retain a brief internal rationale for important exclusions to support consistent operations even where the rule does not require documentation of those out-of-scope assets. Label that record as the organization's management practice. It should not be presented as an additional Level 1 documentation requirement imposed by CMMC.

When Harbor Point begins receiving CUI, the team must reassess the environment using Level 2 rules. A specialized device excluded from Level 1 is not automatically excluded from Level 2. Similarly, the management of security protection services becomes central to the Level 2 asset-category analysis.

5.7 Understand the five Level 2 asset categories

The Level 2 framework distinguishes CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets. Four of these categories are within the assessment scope, with different treatment. Out-of-Scope Assets are outside it when the criteria are satisfied. The category determines how the asset is documented and assessed; it is not merely a label for the inventory. [R1]

A common mistake is to divide every device into either contains CUI or does not contain CUI. That misses assets providing security functions and the other categories in the rule. A monitoring service may have no project drawings while still providing a security capability for the assessed environment. A system that can receive CUI but is not intended to do so may need Contractor Risk Managed treatment rather than an unsupported out-of-scope declaration.

Use the exact regulatory descriptions when reaching a final determination. The following table is a learning summary. It does not replace the fuller conditions, documentation requirements, and assessment treatment in Table 3 of 32 CFR 170.19(c)(1).

Category	Central distinction	Level 2 treatment in brief
CUI Asset	Handles CUI	Document and assess against Level 2 requirements
Security Protection Asset	Provides security functions for the scope	Document and assess relevant capabilities
Contractor Risk Managed Asset	Can handle CUI but is not intended to under established practices	Document treatment with possible limited checks
Specialized Asset	Qualifying specialized equipment unable to be fully secured	Document risk-based treatment and review the SSP
Out-of-Scope Asset	Meets the exclusion criteria and provides no CUI security protection	Be prepared to justify exclusion

Category decisions should be made by people who understand the asset's functions and the governing rules. The inventory administrator can collect facts, but an unsupported automatic label based on operating system, device name, or location will not reliably classify the environment. Record the rationale and the evidence used, especially where the distinction is material to the proposed boundary.

5.8 Identify CUI Assets through actual handling

CUI Assets process, store, or transmit CUI. A system does not have to be the authoritative repository to fit this description. Engineering workstations, servers, application components, storage services, and other assets may qualify according to their actual role. The relevant question is what the asset does with the information in the assessed workflow. [R1]

At Harbor Point, an engineer's managed workstation opens and edits controlled design material. Even if the final version is saved in a cloud repository, the workstation's processing and any permitted local storage must be considered. NorthStar should not describe it as out of scope simply because the company's policy calls the cloud repository the official record.

Backups and restored copies need the same attention. A recovered dataset on a temporary validation server remains information to be handled and protected. If the team restores real CUI to that server, the server's role must be addressed. The word temporary does not create a separate exception to the scoping rules.

Document the asset in relation to the workflow

The inventory entry identifies the asset, owner, location or service context, function, associated information flows, and category rationale. The SSP describes its treatment, and the diagram identifies its place in the scope. The rule requires this coordinated documentation for CUI Assets and preparation for assessment against Level 2 requirements. [R1]

An implementation statement should be specific enough to distinguish the assessed service from another service with a similar name. For a cloud repository, record the relevant tenant, subscription, offering, or other authoritative identifier appropriate to the architecture. A description that says cloud storage is used leaves too much uncertainty for both operations and assessment.

Encryption does not automatically remove an asset from the scoping analysis. The team must evaluate the information handling, applicable rules, service architecture, and any specific authorized treatment. A general claim that all encrypted copies are outside scope is not a defensible substitute for that evaluation.

5.9 Identify Security Protection Assets by their function

Security Protection Assets provide security functions or capabilities to the assessment scope. Their relevance does not depend on holding the customer's engineering documents. Examples may include identity, access management, endpoint protection, vulnerability management, logging, network security, or other components, depending on their actual function in the environment. [R1, R2]

For Harbor Point, the identity service controls who can access the engineering repository. Beacon's monitoring capability receives relevant events and supports detection. NorthStar's configuration management tools help enforce the intended

security settings. Each service must be examined in context rather than being excluded because it is operated by a provider or shared with other customers.

The Level 2 rule calls for Security Protection Assets to be documented in the inventory, SSP, and network diagram. Assessment focuses on the Level 2 requirements relevant to the capabilities provided. This is a functional analysis. It does not mean that every security product is assessed identically or that a one-line invoice establishes the control contribution. [R1]

Follow the management path

If a platform can change firewall policies, disable protection, assign privileged roles, or modify monitoring, determine how that administrative capability is controlled. Who can use it? From which devices? Through which identities and sessions? What is recorded? Can a broad MSP administrator act across customer environments? These questions help establish which components and services support the assessed protection.

Suppose NorthStar moves a customer from one monitoring tenant to another. The project may leave the engineering data untouched, but it changes a security protection service and its evidence. The scope review must consider the new service relationship, configuration, data flow, administration, and responsibility records. A change can affect scope even when no CUI repository moves.

5.10 Distinguish security protection data from CUI

Security Protection Data, or SPD, is security-relevant information used by Security Protection Assets to protect the assessed environment. The rule's examples include relevant configuration, logs, vulnerability information, and passwords granting access to the environment. SPD is not simply another name for all company information or all MSP records. [R2]

NorthStar's firewall configuration may be SPD because it supports protection of Harbor Point's assessed environment. A vulnerability report may have the same relationship. An ordinary billing entry stating that NorthStar provided a support subscription may not have that role. Analyze content and use rather than declaring an entire business application SPD merely from its product category.

Information can require more than one analysis. A security log may contain controlled document content, a sensitive query, or an attached payload. Calling it SPD does not resolve whether it also contains CUI. Review the source configuration,

collection rules, field content, attachments, and downstream processing. A monitoring pipeline should be designed with a clear understanding of what it receives.

Example of a log pipeline decision

Beacon proposes collecting authentication events, device identifiers, and security alerts. NorthStar and Harbor Point review the proposed fields and determine the information involved. They then inspect whether the product also captures command output, file content, screenshots, or diagnostic attachments. The final service description should reflect the enabled collection, not merely the smaller list in the original sales proposal.

Once the team understands the data, it can apply the external-provider rules and define appropriate access, retention, transfer, and evidence handling. Reducing unnecessary collection can simplify operations and exposure, but it must not remove the events or content needed to fulfill the required security function. Data minimization and effective detection need to be evaluated together.

5.11 Use Contractor Risk Managed treatment carefully

Contractor Risk Managed Assets can process, store, or transmit CUI but are not intended to do so because security policies, procedures, and practices are in place. They are in the Level 2 assessment scope. The rule does not require them to be physically or logically separated from CUI Assets, and it provides particular documentation and assessment treatment. [R1]

This category is easy to misuse. A policy that says no CUI here is not convincing if the business process regularly places CUI on the system. If Harbor Point's ordinary collaboration space repeatedly receives controlled drawings during project review, the observed workflow undermines the claim that the established practices prevent that intended use. Correct the workflow and reevaluate the category.

The rule requires inventory, SSP, and diagram documentation and preparation for assessment. When the treatment is sufficiently documented, the assessor reviews the SSP rather than routinely assessing all other requirements on those assets. However, questions raised by the documentation or other findings can lead to limited checks to identify deficiencies, under the conditions specified in the rule. This is not the same as being outside scope. [R1]

Show how the intended restriction operates

NorthStar documents the permitted purpose of an asset, the prohibition or restriction, the people responsible, user instruction, relevant technical measures, and how deviations are identified and addressed. The details depend on the environment. They should explain why the intended use is credible and how ordinary users can perform their work without bypassing it.

An important review question is whether the category remains accurate when an application is added or a team changes its workflow. If a previously general-purpose system becomes a regular CUI destination, update the inventory and implementation plan accordingly. Avoid retaining an old label merely because changing it would increase the work required.

5.12 Recognize Specialized Assets without creating a loophole

Specialized Assets receive specific treatment in the Level 2 rule. The category includes qualifying equipment such as operational technology, test equipment, government-furnished equipment, and certain other identified types that can handle CUI but cannot be fully secured. The organization documents these assets and their treatment, shows risk-based management, and includes them in the diagram. The Level 2 assessment reviews the SSP rather than assessing them against the other CMMC requirements. [R1]

This treatment does not allow the MSP to label every inconvenient server specialized. An ordinary business system does not become test equipment merely because it is old or because patching would disrupt a user. Establish the asset's actual purpose, type, constraints, and basis for the category. Retain the information needed to explain that determination.

Harbor Point uses a measurement device controlled by vendor-specific software. The device's owner explains its role, the information it receives, its supported configuration, and the restrictions on modification. NorthStar evaluates the surrounding connectivity and any intermediate systems. The risk-based treatment might address permitted communications, physical access, maintenance, removable media, monitoring, or other suitable measures. Those measures should fit the actual constraints.

Separate the specialized device from its supporting systems

A specialized instrument may depend on an ordinary file server, maintenance workstation, or identity service. The instrument's category does not automatically transfer to everything connected to it. Evaluate each component's function and information handling. A general-purpose workstation that stages controlled files for the instrument may be a CUI Asset even though the instrument receives specialized treatment.

The Level 3 rules differ from the Level 2 treatment described here. Do not promise a customer that a Level 2 specialized-asset approach will be sufficient for a later Level 3 assessment. If future Level 3 work is plausible, identify that design dependency and address it when reviewing the applicable requirements.

5.13 Justify Out of Scope Assets with evidence

The Level 2 out-of-scope criteria are stronger than not currently storing a project file. The rule describes assets that cannot process, store, or transmit CUI and do not provide security protections for CUI Assets. Physical or logical separation, inherent inability, and the specific VDI condition are relevant to the analysis. An asset that belongs in an in-scope category cannot also be treated as out of scope to avoid assessment. [R1, R2]

NorthStar should be prepared to explain the claimed inability in the implemented environment. The point is not to prove that no imaginable future modification could ever change the device. It is to justify the classification under the actual design, configuration, use, and governing criteria. A guest network with verified separation has a different basis from an ordinary corporate workstation that can freely receive project files but is told not to.

For each material exclusion, record the asset or group, its business purpose, the relevant separation or limitation, and the evidence supporting the conclusion. The rule's table says to prepare to justify the inability; the organization's chosen record is a practical way to preserve that reasoning. Do not present a preferred worksheet format as an official mandated template.

An exclusion example and a failed exclusion

Harbor Point's guest wireless service is separated from the engineering environment and is not used to provide security protection to it. NorthStar verifies the relevant network paths and checks whether guest users have any route through shared

applications or file services. If the facts support the rule's criteria, the team documents its conclusion.

Now consider a corporate file server that is not supposed to hold CUI but is reachable by engineers and routinely receives project exports. The facts do not support simply labeling it out of scope. NorthStar must address the actual information handling and determine the appropriate category. A green rectangle on a diagram does not overcome contradictory evidence.

5.14 Use a repeatable classification workflow

The safest practical starting point is an inventory of facts, followed by a category decision. Record what the asset does, which information it handles, which security functions it provides, how it is connected, and what constraints apply. Then compare those facts with the complete regulatory descriptions. This avoids forcing the environment into categories selected in advance.

For an ordinary asset, first identify actual CUI handling and any security protection role. Next consider whether the specific conditions for another category, including specialized treatment or Contractor Risk Managed treatment, apply. Evaluate an out-of-scope conclusion only when its criteria can be justified. This is a decision aid, not an alternate definition or a rigid priority rule that overrides 32 CFR 170.19.

Some assets have multiple functions. A management server may host security tools while also receiving diagnostic files containing CUI. The classification process must capture both functions and the applicable treatment. Do not choose whichever description appears least demanding and discard the other facts. Obtain qualified review where the combination creates uncertainty.

NorthStar uses a short decision record for difficult cases. The record includes the asset identifier, observed functions, information handled, proposed category, supporting basis, reviewer, approval date, and conditions that would require reevaluation. It links to the inventory and relevant diagram rather than becoming a disconnected spreadsheet.

Decision prompt	Evidence to examine
What does the asset actually do?	Demonstration and configuration
What information reaches it?	Flow records and authorized content review

Decision prompt	Evidence to examine
What protection does it provide?	Service description and control mapping
Which category conditions apply?	Regulatory definition and documented facts
What would invalidate this decision?	Planned changes and known dependencies

Unresolved assets should remain visible in the project plan. Use a provisional status with an owner and required action. Do not quietly treat an unresolved asset as excluded because the inventory report needs a completed category field.

5.15 Compare an enterprise scope with an enclave

An enterprise approach protects and assesses a broad environment that supports the relevant work. An enclave approach establishes a more limited environment for specified information and activities. Either may be appropriate. The decision depends on business workflows, shared services, administration, existing controls, user experience, and the ability to sustain separation over time.

Harbor Point initially considers including its entire corporate environment because engineers already use its email, file shares, and applications. That approach may reduce the need for separate user workflows, but it may bring more assets, legacy applications, locations, and responsibilities into the assessment work. NorthStar must estimate the operating burden as well as the initial remediation effort.

An enclave may reduce the population that directly handles CUI. It may also introduce a separate identity arrangement, restricted exchange process, dedicated endpoints, or virtual desktop service. Those changes can be valuable, but they create administrative and user responsibilities. If employees cannot complete their work inside the enclave, they may move files through unapproved channels and undermine the design.

Compare complete operating models

Evaluate how each option handles engineering work, support, collaboration, backup, printing, software updates, incidents, onboarding, and offboarding. Include the security protection services and provider dependencies. An enclave is not just a

smaller repository; it is an operating environment with a defined way to perform the work.

Consideration	Broader enterprise approach	Defined enclave approach
User workflow	May preserve existing collaboration	May require a separate approved workflow
Remediation	Can involve a larger asset population	May concentrate direct CUI handling
Shared services	Often central to the environment	Still require explicit analysis
Change management	Must track broad organizational changes	Must protect boundary assumptions
Support	Uses established access patterns where suitable	Needs clear restricted support paths

The preferred design is the one the customer can operate correctly and demonstrate. NorthStar should present assumptions and tradeoffs in the decision record rather than promising that an enclave automatically makes most of the company irrelevant to CMMC.

5.16 Prove separation beyond the network diagram

Network segmentation can support a boundary, but the relevant pathways may include more than routed traffic. Shared identities, application permissions, synchronization, backup access, remote administration, file exchange, and removable media can affect how information or control crosses the proposed boundary. The design review should examine each applicable pathway.

Suppose NorthStar separates the engineering workstations from the corporate network using firewall rules. The same engineers can still sign into a corporate file service from those workstations and upload project material. The network design alone has not resolved that information-flow question. The team must consider the application route, approved workflow, controls, and resulting asset treatment.

Shared administration introduces a different concern. A management platform may reach systems on both sides of the boundary and have authority to change security

settings. The analysis should follow its functions, access, and information handling. Do not assume that a separate subnet removes the platform's security protection role.

Test the claims the design makes

NorthStar lists specific claims: corporate devices cannot open the engineering repository; guest devices cannot reach the engineering network; unauthorized users cannot authenticate to the enclave; and prohibited transfer functions are disabled in the selected remote-access design. Each claim receives a test method, expected result, authorized test identity, and evidence record.

Testing must be planned to avoid disrupting production or exposing controlled information. Use approved test accounts and representative noncontrolled test files where possible. A failed test should produce a corrective action and a repeated verification, not a quietly revised diagram that makes the failure disappear.

The result is a documented explanation of separation with supporting configuration and tests. A vulnerability scan may contribute useful evidence, but it does not automatically prove every boundary claim. Match each verification method to the claim being made.

5.17 Evaluate identity and shared administration

Identity services can connect environments that appear separate on a network drawing. Ask which tenant or directory authenticates users, where privileged roles are assigned, how accounts are provisioned, and which recovery paths exist. Then follow the administrators who can change those arrangements. Their authority may be central to the security protection analysis.

Harbor Point proposes using a shared corporate identity service for its enclave. NorthStar evaluates the relevant functions and administrative boundaries. The decision should explain which service components protect the assessed environment, who can alter the policies or group memberships, and how those actions are controlled and evidenced. The fact that the identity service also supports unrelated work does not remove its role.

The team should distinguish a provider's broad internal platform from the specific service contribution and assets relevant to Harbor Point. Shared use may require careful isolation and evidence filtering. It does not necessarily mean that every unrelated customer system becomes part of Harbor Point's assessment. Apply the scoping rules to the actual service and its dependencies.

Include recovery and emergency access

Normal sign-in may use a carefully controlled path while emergency access uses a different account, device, or credential store. Include these arrangements in the design review. The existence of an emergency purpose does not make the access path invisible. Record who can use it, how access is approved or reviewed, and what evidence is retained.

For NorthStar, the administrator credential vault and its access process deserve attention. Where the stored credentials grant access to the assessed environment, the information can be SPD under the rule. The vault's service, administration, and provider relationships must be examined accordingly. [R2]

5.18 Treat remote support as part of the architecture

Remote support is often introduced as a convenience after the enclave design is complete. For an MSP, that order is risky. Support may provide privileged access, file transfer, screen viewing, script execution, clipboard exchange, session recording, and diagnostic collection. Each enabled capability can affect the analysis of information handling and security functions.

Begin with the support task. Does the technician need to view a user's session, administer the operating system, transfer an approved installer, or retrieve a diagnostic file? Use the minimum appropriate capability for that task and document the actual configuration. A product that can transfer files but has that function disabled presents a different factual situation from one routinely used to copy customer documents.

NorthStar traces the technician's device, authentication, management service, connection broker if applicable, target asset, and resulting records. It identifies which systems process or retain session information and whether that information is CUI, SPD, or another type. The review should include the provider's service description and enabled logging or recording features.

A practical support-session walkthrough

The technician receives an approved request through the restricted workflow, authenticates through the designated access method, and connects to the identified customer asset. The customer or authorized service process approves the work according to the agreement. The technician performs the task and records relevant

changes. Temporary access is ended and the evidence is retained in the approved location.

Now introduce a problem: the technician cannot complete the repair without collecting a diagnostic archive. The process should identify an approved exchange and review the archive's information before it enters a different system. Using an ordinary ticket attachment as a shortcut may change both information handling and provider analysis. Design the exception path before a real outage makes the shortcut attractive.

5.19 Examine RMM PSA and documentation platforms separately

Remote monitoring and management platforms, professional services automation systems, and documentation repositories perform different functions. An RMM platform may execute scripts or manage protection. A PSA platform may route tickets, record work, and hold attachments. A documentation repository may store network configurations or credentials. Evaluate each actual use instead of treating the entire MSP stack as one undifferentiated service.

NorthStar's RMM service supports Harbor Point's security configuration and endpoint maintenance. The review examines its administrative access, scripts, command output, stored configuration, and relevant events. Its contribution to the assessed environment should be described in the SSP and provider records as applicable.

The PSA analysis begins with content. A simple request number and scheduling note may be different from a ticket containing a vulnerability report, firewall export, password, or controlled drawing. NorthStar should inspect how technicians use fields and attachments, how email integration copies material, and how retention or search functions preserve it. A written prohibition does not prove that the prohibited content never enters the system.

Design records for the information they need to hold

Harbor Point and NorthStar can use an ordinary ticket to reference a separately controlled evidence location when appropriate, rather than duplicating sensitive content. The reference itself should not disclose more information than necessary. The restricted location still needs its own access, provider, retention, and scoping analysis; moving an attachment does not make the supporting system disappear.

Documentation systems may hold particularly consequential SPD. A network configuration or a credential can enable administration of the environment. Establish

which repository is authoritative, who can export it, how access is reviewed, and how customer information is separated. A generic statement that the MSP keeps documentation in the cloud is insufficient to explain the arrangement.

5.20 Apply the external service provider matrix

The CMMC definition of an External Service Provider concerns external people, technology, or facilities used for IT or cybersecurity services on the organization's behalf, with CUI or SPD processed, stored, or transmitted on the provider's assets. The Level 2 scoping table then distinguishes cloud providers from other providers and distinguishes the information they handle. [R1, R2]

For a cloud service processing, storing, or transmitting CUI, the table points to the FedRAMP requirements in DFARS 252.204-7012. For a noncloud ESP handling CUI, the relevant services are included in the customer's assessment scope and assessed as part of its assessment. For either type handling SPD without CUI, the provided services are in scope and assessed as Security Protection Assets. [R1]

Information handled	Cloud provider treatment	Noncloud ESP treatment
CUI with or without SPD	Apply the referenced FedRAMP requirements	Include the provided services in the customer's assessment
SPD without CUI	Assess the provided services as Security Protection Assets	Assess the provided services as Security Protection Assets
Neither CUI nor SPD	Does not meet this CMMC ESP definition	Does not meet this CMMC ESP definition

The last row does not declare every unrelated vendor secure, nor does it decide all other contractual or asset questions. It answers the particular ESP-definition question in this table. A provider may have other responsibilities under the customer's contract or business arrangements. Keep the decision tied to the rule being applied.

Analyze the service the customer actually uses

A vendor may offer several different services under one company name. One offering may handle CUI, another may hold only SPD, and a third may have no relevant information. Identify the actual service, configuration, data, and relationship. Do not

use a corporate logo or a general compliance statement as a substitute for that analysis.

The rule requires the ESP relationship and provided services to be documented in the customer's SSP and described in the service description and Customer Responsibility Matrix. An ESP may voluntarily undergo certification to reduce its effort during customer assessments; that possibility does not eliminate the need to verify applicability and shared responsibilities. [R1]

5.21 Evaluate cloud offerings at the service level

Cloud-provider evaluation should identify the exact offering and the information it will handle. A provider's general reputation, another customer's authorization, or a different product's status does not establish the status of the selected service. Record the service name and identifiers appropriate to the offering, its boundary, the customer's configuration responsibilities, and the evidence supporting its use.

DFARS 252.204-7012 addresses external cloud services used for covered defense information. It requires security requirements equivalent to the FedRAMP Moderate baseline and the specified incident-related obligations. The scoping rule points to those requirements for CUI-handling CSPs. The customer must evaluate the actual offering and applicable official policy, including any equivalency evidence, rather than accepting a vendor's unsupported use of the word compliant. [R4]

At Harbor Point, the backup provider has a commercial service and a separate offering represented as suitable for the relevant work. NorthStar confirms which service the customer is purchasing. It checks that the contract, technical configuration, responsibility records, and supporting evidence refer to the same offering. A procurement error at this stage can invalidate assumptions made throughout the architecture.

Identify what the customer still implements

A suitable cloud offering does not automatically configure Harbor Point's users, permissions, endpoints, information handling, or incident coordination. The shared responsibility records should identify which protections are inherited and which remain with Harbor Point or NorthStar. Evidence of the provider's contribution must be connected to evidence of the customer's implementation.

Review changes to offerings and features. A new integration, storage location, export function, support option, or subservice may alter data flows or responsibilities.

Require the service owner to evaluate those changes before enabling them in the assessed workflow. The design should remain tied to the service actually used, not the service description that existed at purchase.

5.22 Scope backup restoration and disaster recovery

Backup is a workflow with several components: source data, backup software, transfer paths, storage, management, credentials, job records, and restoration destinations. Some components may handle CUI, while others provide security functions or hold SPD. Describe those roles explicitly. Do not assume that the backup service is outside scope because users do not open its stored copies during ordinary work.

Harbor Point's recovery design identifies where protected copies are retained, who can initiate a restore, what credentials are used, and where restored information may be placed. NorthStar verifies the relevant service configuration and provider analysis. The process also identifies how failed jobs and coverage gaps are detected and resolved.

A restore test can change the information map

Suppose NorthStar tests recovery by restoring a real project folder to a general-purpose laboratory server. That server now handles information it was not intended to receive. The restore procedure should have designated an appropriate destination or used suitable noncontrolled test data where that could meet the test purpose. Review the recovery exercise as part of the data lifecycle, not merely as proof that a backup job succeeded.

Disaster recovery can introduce a different site, provider, network path, identity arrangement, or administrative team. Document these planned operating modes and evaluate their implications before an emergency. A scope that describes only the primary site may fail to explain how the customer protects information during the very event for which the recovery service was purchased.

Retained copies also affect decommissioning. Closing a project folder or deleting a user account does not necessarily remove backup copies, snapshots, or archived exports. The customer needs an authorized retention and disposition process that recognizes those copies and their continuing protection requirements.

5.23 Evaluate virtual desktops against the specific rule

The Level 2 scoping table contains a specific condition for an endpoint hosting a VDI client: the configuration must not allow CUI processing, storage, or transmission beyond the specified keyboard, video, and mouse interaction. Under that condition, the endpoint is considered out of scope. This is a defined treatment for a particular configuration, not a blanket exclusion for all laptops used to connect remotely. [R1]

NorthStar therefore examines clipboard transfer, local drive mapping, downloads, printing, USB redirection, session capture, application integrations, and other relevant capabilities of the proposed design. The question is whether the actual configuration and use satisfy the condition. A remote desktop icon on the workstation does not answer it.

The hosted desktop, applications, storage, identity, connection services, and security functions still require their own analysis. Even when the client endpoint qualifies for the specific treatment, the environment reached through it has not become exempt. Nor does the VDI condition independently resolve personnel, access authorization, information-handling, or contractual responsibilities.

Verify before relying on the exclusion

Using authorized test data, NorthStar checks the prohibited transfer paths, documents the configuration, and reviews user practices. It records the conditions on which the endpoint treatment depends. If a later request enables local printing or file redirection, the change review must revisit the original conclusion before enabling the function.

Avoid extending this rule by analogy to any technology described as browser isolation, remote access, or zero trust. Evaluate the actual service and applicable official guidance. Similar marketing language does not establish identical regulatory treatment.

5.24 Include physical media printing and alternate work sites

Information does not remain inside a logical boundary merely because the repository is well protected. Printing, scanning, copying to removable media, and working at an alternate location can create additional handling paths. A complete scoping discussion includes the people, equipment, facilities, and processes that support those activities.

At Harbor Point, the engineering manager wants printed drawings for review. NorthStar asks which printer will be used, how jobs reach it, whether it stores data, where output is collected, who can access the area, and how paper is retained and destroyed. These questions establish the workflow and the relevant device or specialized-asset analysis; a product name alone cannot determine the category.

If printing is prohibited, verify that the approved workflow is workable and that relevant technical settings support the restriction. Train users on the alternative. A policy that conflicts with an unavoidable business task will encourage exceptions that the architecture has not addressed.

Make remote work concrete

For an authorized home work arrangement, establish the approved device and access method, information storage restrictions, physical handling, screen visibility, printing rules, and incident reporting route. The specific controls should follow the applicable requirements and design. Do not treat remote work as inherently impossible or automatically covered by a cloud subscription.

Visitors and repair personnel can affect physical access to equipment. The customer should understand its role in authorizing entry, supervising relevant activity, controlling keys or badges, and protecting media. NorthStar may configure technology, but it cannot perform all of the customer's local physical responsibilities from its help desk.

5.25 Review collaboration integrations and automated processing

Modern applications can move information without an employee manually downloading a file. Collaboration connectors, workflow automation, search indexing, meeting transcription, and analysis services may receive or generate content. Include enabled integrations in the discovery process and ask what information they access, where they process it, and what they retain.

Harbor Point's project manager proposes connecting the engineering repository to an automated summarization service. The team must analyze the service's actual access and processing before enabling it. The fact that it produces only a short summary does not mean that the source material was never processed elsewhere. The summary itself may also require appropriate handling depending on its content and authority.

The same reasoning applies to meeting features. A discussion of controlled technical details may generate a recording, transcript, chat history, or automatically saved

summary. Review the information, provider, storage, access, and retention arrangements. A meeting link is not a scope decision.

Inventory machine access as well as human access

An integration may use an application identity or API permission that remains active after its original requester leaves. NorthStar records the integration owner, purpose, accessible data, granted permissions, destination service, and review process. Disabling a user's account does not necessarily disable an independent application credential.

Require a change review before adding a new integration to the assessed workflow. The review should confirm the business need, information path, provider treatment, security implementation, and evidence. This creates a practical connection between scoping and application governance without assuming that every new feature is prohibited.

5.26 Build an inventory that supports decisions

An assessment inventory should do more than count computers. It should connect assets to functions, information, owners, categories, relationships, and evidence. The organization may maintain several linked inventories rather than one enormous spreadsheet, provided the records are consistent and another person can follow the connections.

NorthStar separates hardware and virtual assets, applications and services, identities with important administrative roles, and external-provider relationships. Each record has a stable identifier. The data-flow and diagram records use those identifiers so a renamed server or a revised service description does not break the connections between documents.

Start with existing sources: management consoles, purchasing records, application owner lists, network records, cloud subscriptions, and support documentation. Reconcile the sources rather than assuming one is complete. A purchasing list may contain retired equipment; an endpoint console may omit a server that never enrolled; a cloud tenant may contain a trial integration that no longer has an owner.

Use facts that can be maintained

Include fields that have a purpose and an owner. A column requiring a complicated explanation from every technician may become stale quickly. Link to a controlled

category decision or service description when that is more maintainable than duplicating its entire content in every row. The inventory should be detailed enough to support the scope without becoming an unmanageable collection of repeated text.

Inventory field	Why it is useful
Stable asset identifier	Connects inventory diagrams and evidence
Owner and service owner	Assigns business and technical accountability
Function and location	Explains use and operating context
Information handled	Supports CUI and SPD analysis
Category and rationale	Records the scoping decision
Related flows and providers	Exposes dependencies
Verification and review date	Shows the basis and currency of the record

For a group of equivalent workstations, NorthStar may use a common treatment description while retaining individual asset records. It should still be possible to identify which devices were present and managed at the relevant time. Grouping should simplify documentation without concealing differences that affect the scope.

5.27 Create diagrams that explain different relationships

A single diagram overloaded with every user, port, application, control, and provider is difficult to read and difficult to maintain. Use a small set of coordinated views. A logical scope view explains included components and boundaries. A data-flow view explains information movement. An administrative-access view explains who can manage what and through which services.

The diagrams should use consistent asset identifiers, a legend, the scope or system name, an owner, and a version or date. The SSP and inventory should refer to the same components. If the diagram labels a repository HP-REPO-01 while the inventory contains only a generic cloud entry, a reviewer will have to guess whether the records describe the same service.

Explain what each line means

A line may represent a permitted network connection, an application-level transfer, or an administrative relationship. Those are different facts. Label the relationship and keep the diagram's purpose clear. A line from NorthStar to Harbor Point saying support does not explain whether it represents a privileged session, a ticket exchange, a monitoring feed, or all three.

For the data-flow view, show the relevant source and destination, direction, information type, and approved exchange. Supporting records can hold protocols, detailed configurations, and evidence. The diagram should give the reader a reliable overview without requiring every implementation detail to fit in a small box.

For the administrative view, show the credential or identity authority, management platform, target environment, and relevant oversight or logging relationships. This view often reveals why a service outside the engineering subnet still provides a security function within the assessment scope.

Keep the boundary honest

If a provider's relevant service is part of the assessment analysis, represent that relationship even when its infrastructure is offsite. If a corporate service remains connected to the enclave, show the connection and explain its treatment. Do not omit a difficult component to make the picture cleaner. Simplify visual presentation by using linked views, not by removing material facts.

5.28 Write a responsibility matrix people can use

The Customer Responsibility Matrix, or CRM, explains how the customer and provider divide the work associated with the provided services. For an ESP, the scoping rule connects this matrix to the service description and the customer's SSP. The records should explain the actual contribution rather than saying that the provider handles compliance. [R1]

Begin with an operational task or requirement contribution. Identify who makes the business decision, who performs the technical action, who checks the result, and who retains or supplies the evidence. A role can be shared, but the handoff should still be explicit. Shared responsibility without a defined action can become a responsibility that no one performs.

Harbor Point approves repository access. NorthStar configures the approved role and verifies implementation. Harbor Point's designated reviewer evaluates the periodic access review with NorthStar's reports. Beacon may monitor relevant activity but does not decide which engineers have a business need. The matrix should preserve these distinctions.

Activity	Harbor Point	NorthStar or Beacon
Access approval	Defines authorized people and roles	Implements and verifies approved access
Technical change	Approves business impact as assigned	Reviews and performs technical work
Monitoring	Supplies contacts and participates in decisions	Collects reviews and escalates relevant events
Physical access	Operates local facility controls	Supports assigned technology and service duties
Assessment evidence	Owns the assessment record and coordination	Supplies service-specific evidence and expertise

This teaching matrix is intentionally brief. A real CRM needs sufficient detail for the services and objectives involved, with clear interfaces to other providers. One row naming a broad control family rarely explains all of the work necessary to meet that family.

Review the matrix with the personnel who perform the tasks. Ask them to walk through a termination, a security alert, and an urgent change. If the matrix cannot explain those ordinary events, revise it before assessment. The exercise tests whether the document describes a functioning process rather than an agreement in principle.

5.29 Draft a scope statement with explicit assumptions

A scope statement should identify the assessed organization and system, the business work supported, the information involved, the included assets and services, relevant locations, important interfaces, and the basis for exclusions. It should point to the detailed records that support the description. It should also identify unresolved issues rather than burying them in technical appendices.

The statement is not the entire SSP. Its purpose is to orient the reader and establish what the supporting documents describe. The SSP explains the implementation and treatment in greater detail. Inventory, diagrams, data-flow records, and provider documentation supply the connected facts. The scope statement should be concise enough to read as a whole and specific enough to avoid ambiguity.

Sample scope statement for Harbor Point

The following is a fictional example of wording that might be developed after discovery and verification. It is not an approved assessment scope or a template that can be adopted without validation.

Harbor Point Engineering defines the Engineering Collaboration System as the environment supporting the identified engineering subcontract workflow. Authorized engineering personnel receive, process, store, and exchange the project's controlled technical information through the designated exchange service, managed engineering workstations, approved design applications, and controlled repository. The applicable contractual information and assessment requirement are recorded in the contract requirements summary.

The included CUI Assets are identified in the current asset inventory. Security Protection Assets and relevant external services include the identified identity, network protection, endpoint security, vulnerability management, monitoring, and administrative capabilities. Their treatment is described in the SSP and the provider service descriptions. The logical scope, data-flow, and administrative-access diagrams identify the relationships among these components.

NorthStar Managed Technology provides the services specified in the service description and CRM. Beacon SOC provides the identified monitoring and escalation capabilities. Harbor Point retains the business authorization, information-handling, personnel, physical, contractual, and assessment responsibilities assigned to it. Each party supplies and preserves the evidence identified for its contribution.

Corporate systems proposed as outside the scope are identified in the exclusion decision records, with the relevant basis for their treatment. Systems categorized as Contractor Risk Managed Assets or Specialized Assets remain documented and treated according to their applicable Level 2 categories. These categories are not represented as out-of-scope exclusions.

The approved information flows include receipt, engineering processing, controlled collaboration, return of deliverables, backup, authorized restoration, and support

exchanges described in the flow inventory. The design prohibits transfers through unapproved channels and identifies how exceptions and suspected improper transfers are handled. Planned recovery arrangements and approved alternate work practices are documented with the system.

The scope owner maintains this statement and its supporting records through the change-management process. Changes to information, asset functions, providers, administration, locations, integrations, or boundary controls require evaluation before the scope description is relied upon for an assessment or continuing compliance decision.

What must be completed before using this wording

Replace every general reference with the customer's actual controlled record and verified facts. Identify the contract or system records through appropriate identifiers without exposing unnecessary sensitive details. Confirm that the inventory, diagrams, SSP, CRM, and provider evidence support the statement. A polished paragraph cannot compensate for incomplete discovery or an untested exclusion.

5.30 Verify the scope before the assessment

A scope review should test consistency and behavior. Start by comparing the inventory, SSP, diagrams, provider list, responsibility records, and data-flow descriptions. Then use authorized demonstrations and tests to verify important claims. The aim is to discover contradictions before an assessor or an incident exposes them.

NorthStar selects representative workflows, including normal engineering activity, remote support, backup, restoration, access removal, and a prohibited transfer. It records the test identity, relevant assets, approved test data, expected result, observed result, and evidence. The test should be reproducible enough for another qualified person to understand what was established.

Test	Expected result	Evidence
Unauthorized corporate access	Repository access denied	Permission record and observed denial
Approved engineering work	Authorized task succeeds in the designated environment	Workflow demonstration

Test	Expected result	Evidence
Guest network isolation	Prohibited network paths unavailable	Configuration and test result
Restricted remote transfer	Disabled function cannot move the test file	Session settings and observed behavior
Approved restoration	Data restored only to the authorized destination	Restore request and result

Explain the limits of a successful test

One successful denial does not prove that every possible path is blocked. Select tests based on the architecture and the actual boundary claims, and review coverage. A test of one user may not evaluate an administrator, an application identity, or a legacy protocol. A network test may not evaluate cloud sharing permissions. The report should state what was tested and what remains dependent on other evidence.

When a test fails, identify whether the cause is an implementation problem, an inaccurate document, or an incorrect design assumption. Each calls for a different correction. Fix the relevant cause, update the supporting records, repeat the verification, and obtain the appropriate review. Do not classify the failure as an assessor misunderstanding before checking the facts.

5.31 Work through the Harbor Point scoping engagement

We will now combine the method into one extended example. Harbor Point has a corporate office, engineers who sometimes work remotely, a design application, several existing cloud services, and NorthStar's shared support stack. The customer expects to handle CUI for an identified project and wants a defined environment. The project does not assume a universal certification deadline; Harbor Point confirms the actual requirement and current direction before scheduling assessment work.

Discovery reveals a broader workflow

The first meeting identifies eight engineers and two reviewers. The project manager initially says that all files stay in the engineering repository. During a demonstration, an engineer downloads a file to the workstation, edits it locally, and sends a screenshot to a reviewer through an ordinary collaboration channel. NorthStar records the actual steps and asks the customer to decide which workflow will be approved.

The backup review finds that the existing service captures workstation folders as well as the repository. The support review finds that technicians sometimes attach diagnostic archives to ordinary tickets. Neither fact is treated as a minor documentation issue. Both create information paths that must be understood and addressed before the scope can be finalized.

Harbor Point assigns owners to unresolved questions: the project manager confirms the information and authorized exchanges; the application owner verifies local file behavior; NorthStar examines support and backup configurations; Beacon describes the monitoring fields and retention. Each answer updates the same set of flow and service records.

The first architecture option is rejected

NorthStar's initial sketch places the repository in an enclave but leaves the same broad file-sharing and support practices in place. The team recognizes that the drawing is narrower than the operating process. It rejects the sketch as an incomplete design rather than presenting it as a finished scope.

The revised proposal defines the approved engineering workstations, application behavior, repository, exchange method, support path, and recovery destination. It restricts the relevant cross-boundary functions and documents the remaining shared services. Harbor Point reviews the effect on the engineers' work before accepting the design. The customer must be able to complete legitimate tasks through the approved process.

The asset review distinguishes function from ownership

The managed engineering workstations and repository handle CUI. The identified identity and monitoring services provide security capabilities. Corporate assets are evaluated individually or in justified groups rather than automatically excluded. A measurement device receives a separate specialized-asset review. The team does not assign the device's category to its ordinary supporting workstation without examining that workstation's role.

NorthStar's management platform is external to Harbor Point and shared with other customers. The team examines its relevant service contribution, administrative access, and information handling. It plans how NorthStar will provide customer-specific evidence without disclosing unrelated customers' records. Shared use is addressed as an architecture and responsibility issue, not as a reason to omit the service.

Provider review changes the purchasing decision

The proposed backup order refers to the provider's standard commercial product, while the architecture assumes a different offering. NorthStar detects the mismatch by comparing the order, service description, and technical setup. Harbor Point corrects the purchasing decision and confirms the evidence and shared responsibilities for the selected offering before using it for the protected workflow.

Beacon's proposed log collection initially includes a diagnostic field whose contents have not been evaluated. The parties inspect its behavior and decide how the field will be handled. The service description is updated to match the final collection. They do not rely on a general assertion that logs never contain CUI.

Boundary tests expose two remaining problems

The first test confirms that an unauthorized corporate user cannot open the repository. A second test finds that an application integration can still export files using an old permission grant. NorthStar removes or revises the integration as authorized, verifies the new behavior, and updates the application-access inventory. The first successful user test had not established that machine access was restricted.

The remote-support test finds that clipboard transfer is disabled but file transfer remains available. The proposed VDI or remote-client treatment must be evaluated against the actual design and rule; partial restriction is not assumed to satisfy it. NorthStar corrects the configuration or revises the scope decision, then documents the verified result.

Management receives a decision package

Harbor Point's scope owner reviews the final statement, inventories, diagrams, service descriptions, CRM, exclusion rationales, unresolved issues, and verification results. The package identifies what has been established and what still requires action. The customer approves its business and operational decisions, while the technical owners confirm their implementation responsibilities.

This internal approval does not guarantee an assessor's acceptance or establish a CMMC status. It establishes a coherent, reviewed basis for the next stage of work. The organization can now explain the environment, demonstrate important claims, and answer questions without reconstructing its architecture from scattered tickets.

The engagement continues after the drawing is signed

A month later, Harbor Point adds a reviewer who works from another location. NorthStar checks the approved access method, device, information handling, physical responsibilities, and role before granting access. The records are updated where necessary. The scope remains a controlled operating description rather than a historical project artifact.

The example illustrates a useful measure of success: when someone asks why an asset is included or excluded, the answer can be traced to facts, a rule, an approved decision, and evidence. The team does not need to rely on the memory of the engineer who drew the first diagram.

5.32 Maintain scope through a defined change process

Scope can become inaccurate without a major network redesign. A new application, integration, backup destination, service account, office, support feature, or provider can change the information or protection relationships. Build a scoping question into the ordinary change process so these events receive review while the decision is still reversible.

NorthStar's change record asks whether the proposed work changes information handling, a security function, a provider, an administrative path, a location, or an exclusion assumption. A positive answer triggers review by the appropriate scope and technical owners. The result may require updated records, testing, a revised implementation, or further qualified assessment advice.

Do not assert that every routine change automatically requires a new assessment. Evaluate the significance under the applicable rules and contractual requirements. Likewise, do not assume that a previously assessed environment remains adequately described after a material change. The scope owner needs a documented basis for the decision and appropriate escalation when the effect is uncertain.

A practical change sequence

Describe the proposed change and its business purpose. Identify affected assets, flows, providers, and responsibilities. Evaluate the intended category and control treatment. Obtain authorization, implement the change, verify relevant behavior, and update the scope records. Finally, confirm that evidence and operating procedures reflect the new arrangement.

Harbor Point's request to enable a new file-export feature illustrates the sequence. The application owner explains the purpose; NorthStar identifies the destination and permissions; the customer evaluates the information and provider implications; the team authorizes and tests an appropriate configuration. Enabling the feature first and documenting it months later reverses the control process.

5.33 Manage multiple customers locations and business changes

An MSP needs a repeatable method without assuming that every customer has the same scope. NorthStar can standardize discovery questions, inventory fields, evidence practices, and reference architectures. It must still identify each customer's information, contract, system, providers, and responsibilities. A standard service package is an input to the analysis, not a completed customer scope.

Shared platforms require customer-specific views and access boundaries. The MSP should be able to identify Harbor Point's relevant assets, settings, records, and service contribution. It should also understand which platform-level functions affect more than one customer. This helps the MSP coordinate changes and evidence while protecting unrelated customer information.

A merger or new office deserves more than an inventory update

If Harbor Point acquires another business, the project may introduce users, applications, networks, contracts, providers, and records with different handling requirements. Connecting the networks before assessing these relationships can create information and administrative paths that the original scope never considered. Review the proposed integration before relying on the old boundary.

For an additional office, evaluate physical responsibilities, access, local equipment, printing, connectivity, support, and information movement. A site does not need to host a server to affect the assessed workflow. Conversely, the existence of another location does not by itself prove that every asset there receives identical treatment. Follow the functions and information.

Offboarding a provider also changes the architecture. The customer needs its records, configurations, evidence, and access under an agreed transition process. Revoke obsolete provider access, verify replacement services, and preserve required historical records. The assessment documentation should remain usable after the original MSP is no longer operating the environment.

5.34 Recognize the most common scoping mistakes

Starting with a price instead of a workflow

An assessment budget is a legitimate business constraint, but it does not determine which assets meet a regulatory category. Begin with facts, then compare viable designs and their costs. If the affordable option requires a different workflow, the customer must approve and implement that workflow before relying on its boundary.

Treating a policy as proof of impossibility

A no-CUI policy may be part of Contractor Risk Managed treatment where the conditions are met. It does not automatically establish the stronger out-of-scope criteria. Review what the system can do, how it is actually used, and what the implemented practices support.

Ignoring the MSP because it is offsite

Remote administration, identity, security monitoring, configuration data, and credentials can make provider services relevant. Follow the service and information relationships instead of using the customer's office walls as the assessment boundary.

Assuming a cloud service removes customer duties

The provider's applicable status and evidence address its contribution. The customer and MSP still need to implement and demonstrate their assigned responsibilities. Verify the selected offering and the configuration used, then connect inherited protections to the customer's actual implementation.

Using a broad technology label as a category

Cloud, VDI, OT, RMM, and zero trust describe technologies or services, not automatic final scope determinations. Apply the relevant rule to the actual functions, data, constraints, and configuration. A product description is not an assessment conclusion.

Forgetting temporary and emergency workflows

Recovery servers, diagnostic transfers, vendor maintenance, and emergency access can create material paths. Include the authorized operating modes and explain how they remain controlled. The environment should still make sense when an ordinary failure occurs.

Allowing the records to disagree

An inventory that includes a service omitted from the diagram, an SSP naming a retired platform, and a CRM assigning work to an obsolete provider create uncertainty. Reconcile the documents and assign an owner to keep them current. Consistency supports both operations and assessment.

5.35 Practice the decisions with worked scenarios

Scenario 1 The corporate workstation with a project copy

An engineer uses a corporate workstation to open a controlled drawing and then deletes the file. The team had labeled the workstation out of scope. The actual processing contradicts the simple exclusion claim. Investigate the workflow, any retained copies, and applicable handling obligations. Then determine the proper treatment and correct either the workflow or the scope. Deletion alone does not establish that the earlier handling never occurred.

Scenario 2 The SOC that says it never receives CUI

Beacon collects events and vulnerability information used to protect the assessed environment. Even if those records contain no CUI, they may be SPD, and the provider's relevant services receive the applicable Security Protection Asset treatment. Verify the fields and attachments before accepting the no-CUI claim. The correct conclusion depends on the service's actual information and role, not on the word SOC.

Scenario 3 The guest network with a shared application

Network tests show that guest devices cannot reach the engineering subnet, but an application sharing link permits access to a project repository. The network test established only one part of the boundary. Review application access and the resulting information path, correct the inappropriate access, and repeat the relevant verification. Do not claim complete separation from the network result alone.

Scenario 4 The device called specialized because it is old

A general-purpose server is difficult to patch, so its owner proposes Specialized Asset treatment. Age and inconvenience alone do not establish that category. Determine the server's actual type, function, constraints, and information handling against the rule. If it does not qualify, the organization must address its real category and implementation needs rather than using a label to defer the work.

Scenario 5 The virtual desktop with local printing

NorthStar proposes treating a client endpoint as out of scope under the specific VDI condition, but local printing is enabled. The team must evaluate that configuration against the condition rather than assuming that remote display is sufficient. Either implement and verify a qualifying design or revise the treatment based on the actual information handling and functions.

Scenario 6 The approved provider with the wrong offering

Harbor Point's architecture references one cloud offering, but purchasing ordered another. Pause use of the mismatched service for the protected workflow while the customer resolves the issue. Verify the selected service, contractual requirements, evidence, and configuration. A provider's status for one offering does not automatically apply to every product it sells.

Scenario 7 The support ticket with a password

A technician enters a credential granting access to the assessed environment into an ordinary ticket. The credential is relevant to the SPD analysis, and the event may also require immediate credential and information-handling action. Use the approved response process, investigate retained copies and access, and correct the support workflow. Do not assume that changing the ticket field removes every copy or every consequence.

Scenario 8 The excluded asset that becomes a security service

A corporate server is repurposed to collect and analyze security events for the enclave. Its new function changes the analysis even if it does not receive project documents. Review its Security Protection Asset role, associated SPD, administration, and documentation. An old out-of-scope label should not survive a material change in function without review.

Scenario 9 The restore into a laboratory

An administrator restores controlled project data into a general laboratory for a recovery test. The laboratory's intended purpose does not negate the actual information handling. Protect the data, follow the relevant response and corrective process, and evaluate the affected assets and providers. Redesign the test to use an approved destination and appropriate data.

Scenario 10 The shared identity platform

The enclave and corporate systems use the same identity service. That fact does not establish that every corporate asset has the same category, but it does require analysis of the identity service's security role and administration. Identify relevant policies, privileged roles, recovery paths, and responsibilities. The scope should explain how the shared service supports the assessed environment.

Scenario 11 The subcontractor receiving only FCI

A subcontractor receives information for a limited task and believes the prime contractor's Level 2 environment determines its own entire scope. Review what the subcontractor actually receives, generates, and handles, along with the applicable flowdown. Do not copy the prime's asset list or assume identical information. The appropriate contractual requirement and scoping rules must be established for the subcontractor's own work.

Scenario 12 The assessor asks about an omitted provider

During preparation, a reviewer finds a monitoring provider in a service invoice but not in the SSP. NorthStar should establish what the provider actually does and which information it handles, then correct the records and implementation as necessary. The invoice alone does not prove the category, but it identifies a discovery gap that deserves resolution before the scope is presented as complete.

5.36 Conduct a scoping workshop with the customer

A practical workshop turns the chapter into a coordinated set of decisions. Include the business owner, relevant users, system owner, MSP technical lead, and provider representatives where needed. Bring the existing contract requirements summary, inventories, diagrams, service descriptions, and known information-flow records. Use authorized examples and protect the material discussed.

Begin with one complete workflow. Ask the employee to explain receipt, processing, sharing, retention, backup, support, and disposal. Record the assets and services involved. Identify uncertainties without trying to settle every technical question in the meeting. Assign each unresolved item to a person who can obtain evidence or authoritative clarification.

Next, review the proposed categories and provider treatment. For each significant asset, ask what facts support the determination and what would invalidate it. Give

particular attention to proposed exclusions, shared security services, specialized equipment, and integrations. The workshop should expose assumptions before those assumptions become commitments in a statement of work.

Build the package in a controlled sequence

1. Confirm the business work information and applicable requirement.
2. Document the complete approved workflow and meaningful exceptions.
3. Reconcile assets services identities and provider relationships.
4. Apply category and provider rules with recorded rationales.
5. Develop the coordinated scope statement SSP references diagrams and CRM.
6. Verify important claims and resolve material gaps.
7. Obtain the appropriate internal review and assign ongoing ownership.

The outputs should be useful after the workshop. NorthStar provides a decision list, unresolved items, owners, and the next required evidence or test. Harbor Point confirms its business decisions and assigns customer actions. Avoid ending with only a diagram and a general statement that everyone agrees.

Use an exit review before declaring readiness

Ask whether the significant information paths are understood, every material asset and provider has been addressed, exclusions have a defensible basis, responsibilities are assigned, and the records agree. Confirm that known failed tests have been corrected and retested. Where an issue remains unresolved, state its effect on the readiness conclusion.

An internal exit review does not replace the formal assessment. It gives the organization a credible basis for proceeding and reduces the chance that assessment time will be consumed discovering the environment. The workshop succeeds when the customer and MSP can explain the system together and identify who maintains each part of that explanation.

5.37 Chapter Review and Application

Scoping begins with business work and information handling, then follows the assets and services that perform and protect that work. The Level 2 categories distinguish direct CUI handling, security protection, contractor risk management, specialized

equipment, and defensible exclusions. These categories have different treatment and should not be collapsed into a simple list of computers that contain documents.

For an MSP, provider relationships and administrative pathways are central. RMM, monitoring, identity, credentials, support records, backup, and cloud offerings may introduce information or security functions that must be explained. Evaluate each actual service and its enabled behavior. Neither an offsite location nor a broad vendor claim resolves the scoping question.

The scope statement, inventory, diagrams, SSP, CRM, provider records, and verification results should tell the same story. When ordinary changes occur, the organization should be able to update that story through a defined process. A scope that depends on one engineer's memory is difficult to operate and difficult to defend.

Review Questions

1. How does an assessment scope differ from an MSP's service agreement?

2. Why should discovery begin with a business workflow rather than a device count?

3. Which hidden copies can an ordinary application or support process create?

4. What distinguishes a CUI Asset from a Security Protection Asset?

5. Why does a no-CUI policy not automatically establish an out-of-scope asset?

6. What treatment does a Level 2 Contractor Risk Managed Asset receive?

7. Why should specialized equipment and its supporting workstation be evaluated separately?

8. What information can qualify as SPD even when it contains no project documents?

9. How does the external-provider analysis differ for CUI and SPD-only services?

10. What must be checked before relying on the specific VDI endpoint condition?

11. How can a successful network test leave an application-level path untested?

12. What should a scope change review consider when a new integration is proposed?

Answer Guidance

For Questions 1 through 3, connect responsibility, activity, and information. A service agreement divides work between parties; it does not remove the customer's assessment obligations. The workflow identifies what systems actually do, including

temporary and retained copies that a hardware list cannot reveal. A strong answer follows a particular file or activity rather than reciting a general principle.

For Questions 4 through 7, explain the category criteria and treatment. Direct CUI handling and security protection are different functions. Contractor Risk Managed Assets remain in scope under their specific treatment, while an out-of-scope conclusion needs its own basis. Specialized treatment depends on qualifying facts and does not automatically extend to ordinary connected equipment.

For Questions 8 through 10, focus on data content and service behavior. Configuration, relevant logs, vulnerabilities, and access credentials can be SPD. Provider analysis follows both information type and provider type. The VDI condition depends on the implemented restrictions, not on the presence of a remote desktop client or a vendor's product label.

For Questions 11 and 12, explain verification coverage and change impact. Different tests establish different claims. An integration can introduce a new destination, application permission, provider, or retained copy even if the network remains unchanged. Review those relationships and update the records before relying on the original boundary.

An applied exercise

Choose a fictional MSP customer with six engineers, a corporate office, remote work, a design application, cloud storage, backup, and external monitoring. Describe one complete CUI workflow. Create a proposed inventory with category rationales, identify at least three provider or security protection questions, and describe two assets that might be excluded only after further verification.

Write a scope statement of several connected paragraphs and list the supporting records it requires. Then propose five tests, each tied to a particular claim. Introduce one failed test and explain whether it requires a configuration correction, a documentation correction, a different category, or a redesign. More than one action may be necessary.

Finally, add a new office or a support integration. Identify the decisions, records, and verification that must change. The exercise is complete when another reader can follow why each material component receives its proposed treatment and where the supporting evidence would be found.

Key Terms

Term	Meaning in this chapter
Assessment scope	Assets receiving the applicable CMMC assessment treatment
CUI Asset	Asset that processes stores or transmits CUI
Security Protection Asset	Asset providing a security function for the assessed scope
SPD	Security-relevant data used to protect the assessed environment
Contractor Risk Managed Asset	Asset capable of CUI handling but not intended for it under established practices
Specialized Asset	Qualifying equipment receiving the rule's specialized treatment
Out-of-Scope Asset	Asset meeting the applicable exclusion criteria
ESP	External IT or cybersecurity service provider meeting the CMMC definition
CSP	Provider of cloud services under the applicable definition
CRM	Record describing customer and provider responsibilities
Data-flow record	Description of a meaningful information movement and its context
Scope owner	Assigned role maintaining the scope and coordinating changes

Closing Perspective

An MSP that can explain a customer's scope accurately has established the foundation for the remaining readiness work. The team knows which environment it is protecting, who participates, where information moves, and which decisions must remain controlled. That understanding allows implementation and evidence work to proceed against a coherent system rather than a collection of assumptions.

The practical standard is whether the customer and MSP can answer four connected questions: what is included, why it is included, how it is protected, and what evidence supports the description. When they can answer those questions consistently through routine operations and change, the scope becomes a useful management tool as well as an assessment requirement.

Official References

R1. 32 CFR 170.19, CMMC scoping, including Level 1 differences, Level 2 asset categories, ESP treatment, and Level 3 differences. Official annual CFR edition. Read official source

R2. 32 CFR 170.4, Acronyms and definitions, including assessment scope, ESP, CSP, Security Protection Assets, SPD, and Out-of-Scope Assets. Read official source

R3. National Archives and Records Administration, CUI Registry. Categories and associated controlling authorities. Read official source

R4. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. See the external cloud provisions and related incident obligations. Read official source

R5. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Archived NIST edition incorporated into the published CMMC Level 2 baseline discussed here. Read official source

R6. Electronic Code of Federal Regulations, 32 CFR Part 170. Consult the current rule for amendments to the annual CFR text cited above. Read official source

R7. Official CMMC program page, including the July 13, 2026 announcement regarding Phase II suspension and continuation of Phase I self-assessment requirements. Check this source and applicable contracting direction for subsequent developments. Read official source

Source review date September 19, 2026. The detailed scoping explanations use the identified official rule text. Program rollout direction and contractual applicability require a current check before a customer relies on a deadline or assessment commitment. The fictional examples illustrate the method and do not constitute official scope determinations.

CMMC for MSPs

From Readiness to Certification

Chapter 6

Building the CMMC Responsibility Matrix

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and source context — 3

6.1–6.8 Foundations and responsibility design — 4

6.9–6.11 Objectives, activity records, and handoffs — 13

6.12–6.17 Access, logging, monitoring, and incidents — 17

6.18–6.21 Vulnerabilities, changes, integrity, and recovery — 24

6.22–6.26 People, facilities, media, and assessment — 28

6.27–6.31 Providers, inheritance, evidence, and agreements — 32

6.32 Harbor Point responsibility matrix case study — 38

6.33–6.35 Validation, maintenance, and common failures — 41

6.36–6.37 Scenarios, workshop, and chapter review — 45

Official references — 52

Chapter Purpose

A customer can know exactly which systems belong in its CMMC assessment scope and still have a serious operational problem: the people protecting those systems may disagree about who is supposed to do the work. The customer assumes that the MSP reviews access. The MSP assumes that the department manager reviews access. The cloud service supplies a report, but nobody reads it. Each participant can describe a service, yet the complete security activity remains unfinished.

In this chapter, we will turn those assumptions into explicit responsibilities. We will build a responsibility matrix that identifies the work, the authority to approve it, the people who perform it, the evidence it produces, and the action required when something goes wrong. We will also connect the matrix to the actual assessment scope, the system security plan, provider service descriptions, operating procedures, and service agreements. The goal is a document that people can use during ordinary operations as well as during assessment preparation.

The central lesson is that assigning a name to a requirement does not establish that the requirement is implemented. An effective matrix explains a working relationship. It shows where the customer's decision ends, where the provider's action begins, and how the organization confirms that the intended result occurred. When the work crosses several organizations, those handoffs deserve as much attention as the individual technical tasks.

We continue the fictional Harbor Point Engineering engagement introduced in earlier chapters. NorthStar Managed Technology provides managed IT services, Beacon SOC provides an agreed monitoring service, and a cloud provider supplies selected infrastructure or application capabilities. The examples, identifiers, schedules, and service arrangements are teaching material. They illustrate how to reason through responsibilities; they are not an official CMMC matrix, an approved customer implementation, or a complete assessment package.

Learning Objectives

- Distinguish the regulatory customer responsibility matrix from a general project assignment chart.
- Separate decision authority, implementation, operation, verification, and evidence custody.
- Translate security requirements and assessment objectives into manageable activities.

- Explain customer, MSP, security provider, and cloud provider contributions without overstating inheritance.
- Build responsibility records for access, monitoring, configuration, incidents, personnel, physical protection, and documentation.
- Resolve missing owners, contradictory agreements, weak handoffs, and unavailable provider evidence.
- Validate and maintain a matrix through operational walkthroughs, service changes, and assessment preparation.

Source and Applicability Note

This chapter uses the published CMMC framework in 32 CFR Part 170, particularly the provisions addressing external services, assessment evidence, and affirmation. Level 2 examples refer to NIST SP 800-171 Revision 2 and the June 2018 NIST SP 800-171A assessment publication incorporated into that framework. A newer NIST publication should not be substituted simply because its publication date is later. Confirm the requirements incorporated by the applicable rule and contract. [R1, R2, R3, R4]

The chapter concentrates on responsibility design rather than acquisition rollout dates. Determine the customer's actual required assessment type and contractual obligations from current official direction. Sample review intervals, task labels, approval practices, and record formats are management examples unless the text expressly identifies a governing requirement. A responsibility matrix cannot change a regulation, waive a contractual obligation, or establish a CMMC result by itself.

6.1 Begin with the Work That Falls Between Organizations

Let us begin with a familiar service desk situation. Harbor Point hires a new engineer. Human resources sends a message to NorthStar asking for an account. The technician creates it and copies the permissions of another engineer. The employee can sign in, the application opens, and the ticket is closed. From a service desk perspective, the request appears successful.

Now ask a different set of questions. Who decided that the new engineer should have access to the controlled project? Who approved the specific role? Was the copied account an appropriate model, or did it contain permissions accumulated over several projects? Who verified that the new account could perform authorized work without

receiving unnecessary access? Where is the evidence connecting the approved request to the implemented permissions?

These questions reveal the difference between completing a technical request and completing an authorized security process. NorthStar may have performed every technical action requested of it while the customer failed to provide a necessary authorization. Alternatively, the customer may have supplied a valid authorization that the technician interpreted too broadly. The matrix must make both contributions visible.

A similar gap can occur after a monitoring alert. Beacon detects unusual activity and sends a notification. NorthStar believes Harbor Point must authorize containment. Harbor Point believes the monitoring subscription includes immediate containment. The delay is not caused by a missing security product. It results from an unresolved decision about authority and action.

The first purpose of responsibility mapping is therefore discovery. Before filling in cells, ask participants to explain how ordinary work actually moves among them. Look for phrases such as someone should, normally they handle it, or we thought that was included. These statements are useful evidence of ambiguity. They identify decisions the engagement needs to resolve before the customer relies on the process.

Follow One Event from Beginning to End

Choose an event with a clear beginning and a result that can be observed. An employee joining, a privileged role changing, a vulnerability appearing, or a backup restoration request works well. Have each participant explain what information it receives, what it does, what it produces, and who acts next. Do not stop when the first organization finishes its portion.

At Harbor Point, this exercise shows that the account request process has an implementation step but lacks a documented access decision and a verification step. The team can now correct a specific weakness. It does not need a vague instruction to improve accountability; it needs a named approver, a defined request, an implementation procedure, and a reliable completion check.

6.2 Understand What the CMMC Customer Responsibility Matrix Describes

The CMMC scoping rule connects external services to the organization's system security plan and to the provider's service description and customer responsibility

matrix. The CRM describes the responsibilities of the organization seeking assessment and the external service provider with respect to the services provided. This relationship matters because a customer may rely on security functions performed outside its own facilities or direct administrative control. [R1]

A provider's CRM is consequently more than an internal staffing chart. It explains which aspects of a service the provider performs and which duties remain with the customer. For example, a cloud service may operate the underlying platform while the customer must configure tenant access, identify authorized users, and manage its own information. An MSP may perform some of those customer-side technical duties under a separate agreement. The complete arrangement must connect these layers.

Different organizations use names such as shared responsibility matrix, customer responsibility matrix, or control responsibility matrix. The name alone does not establish completeness. Read the document to determine whether it describes the actual offering, the customer's implementation, the relevant security responsibilities, and the boundaries between participants.

Harbor Point uses one coordinated customer matrix and retains the relevant provider CRMs as supporting sources. Its coordinated matrix does not rewrite a cloud provider's obligations. Instead, it explains how Harbor Point and NorthStar perform the duties that the cloud provider assigns to the customer, while identifying the provider contribution that the implementation relies upon.

The rule should not be interpreted as prescribing every column shown in this chapter. Fields such as trigger, verifier, evidence location, and escalation route are practical ways to make the required relationship understandable and operational. Their value comes from the decisions they expose, not from matching a fictional spreadsheet format.

A Matrix Can Be Accurate and Still Be Incomplete

Suppose a provider correctly states that the customer is responsible for assigning application roles. That statement may be accurate at the provider boundary. Harbor Point still needs to determine whether its engineering manager approves the role, NorthStar configures it, and a designated reviewer checks the result. The provider's statement starts the customer-side discussion; it does not finish it.

Similarly, a matrix that identifies all technical operators may omit business decisions, personnel processes, facility tasks, or evidence responsibilities. Those omissions matter because the assessed environment depends on more than the technologies

listed in the MSP proposal. The customer needs a coordinated explanation of the complete service relationship.

6.3 Distinguish the Matrix from the Other Documents

The responsibility matrix works alongside several records that serve different purposes. The assessment scope identifies the environment being assessed. The SSP describes the environment, how requirements are implemented, and relevant relationships. A procedure explains how an activity is performed. A service agreement establishes the commercial commitments between parties. Evidence records what actually happened. The matrix connects the people and organizations that maintain this arrangement. [R1, R3]

Confusion arises when one document is expected to do all of these jobs. A technician may point to a contract saying endpoint management is included, but the contract may not explain who approves an exception. A policy may require access review without assigning responsibility for producing the account list. An SSP may describe a monitoring capability without identifying who responds when that capability stops receiving events.

Harbor Point avoids repeating every procedure inside its matrix. Each row describes the responsibility clearly enough to identify the activity and then refers to the controlled procedure or supporting record. This reduces duplicate instructions that may drift apart over time. The references must be meaningful, however. See policy is not sufficient when the organization has several policies and none describes the relevant handoff.

Record	Main question answered	Relationship to the matrix
Assessment scope	What environment is being assessed?	Defines the systems and services to which assignments apply
SSP	How are requirements implemented?	Explains the implementation supported by the assignments
Provider service description	What service is actually supplied?	Establishes the provider contribution and limitations

Record	Main question answered	Relationship to the matrix
Service agreement	What work has been agreed?	Supports the authority and resources needed for the assignments
Operating procedure	How is the work performed?	Supplies steps referenced by the activity record
Evidence record	What happened and what was observed?	Supports verification of the assigned work

Reconcile Disagreement at the Source

If NorthStar's service agreement excludes application administration but the matrix assigns NorthStar all application access tasks, do not quietly choose one document as the truth. Investigate the intended arrangement. The service may need to be added, the customer may need to retain the task, or a different provider may need to perform it. Update the affected records through the appropriate approval process.

A signed matrix can be useful evidence of an agreed allocation. It does not automatically amend every underlying agreement or prove that the assigned party has the necessary access and resources. The organization should be able to explain why each assignment is both authorized and practical.

6.4 Separate Authority from Execution

Responsibility discussions often use the word owner without defining it. One participant means the person who approves a decision. Another means the person who performs the technical task. A third means the person who maintains the evidence. When these meanings are mixed, a cell containing one name can hide several unassigned activities.

For this chapter, decision authority means the role permitted to approve the business or security decision involved. Execution means performing the authorized work. Verification means checking that the intended result was achieved. Evidence custody means maintaining the records needed to explain and demonstrate that result. These are practical distinctions, not additional official CMMC role titles.

At Harbor Point, the engineering manager decides whether an employee needs access to a project. NorthStar implements the approved role. A designated reviewer checks that the implemented permissions match the decision. Harbor Point's controlled evidence repository retains the authorization and the implementation record, with NorthStar contributing the technical evidence. The same person may perform more than one role where appropriate, but the duties remain distinct.

This distinction becomes especially important when a provider has powerful administrative access. A technician's ability to change a permission does not establish the business authority to approve that permission. Conversely, a manager's approval does not prove that the change occurred. The workflow needs both an authorized decision and a completed action.

Keep Organizational Accountability Visible

Outsourcing tasks does not remove the customer's obligation to satisfy the requirements that apply to its assessed environment. The CMMC affirmation provisions identify an Affirming Official who is a senior representative within the organization, with the authority and responsibility described in the rule. An external provider can prepare information and support the process, but the matrix should not casually designate an outside technician as the customer's Affirming Official. [R5]

Harbor Point therefore distinguishes its internal executive oversight from NorthStar's service delivery accountability. NorthStar is accountable for meeting its agreed commitments; Harbor Point remains responsible for its own business decisions and applicable CMMC obligations. This is compatible with extensive outsourcing, provided the allocation is explicit and supported by the actual arrangement.

6.5 Use RACI Only When It Clarifies the Work

RACI is a common assignment convention: responsible, accountable, consulted, and informed. It can be useful for showing who performs work, who owns an outcome, whose input is needed, and who receives updates. CMMC does not become a RACI exercise merely because the letters fit neatly into a spreadsheet. The convention must serve the real responsibility description.

A high-level row labeled access control with the customer marked accountable and the MSP marked responsible is a starting point. It does not explain who identifies authorized users, approves role changes, removes access after termination, manages

application identities, or verifies restrictions. Broad RACI rows should lead to the activity-level detail needed by the environment.

When NorthStar uses RACI internally, it defines the letters at the beginning of the document. It also avoids giving the same letter incompatible meanings in different tables. If accountable means the internal outcome owner in one place and the contractual provider in another, readers cannot interpret the chart reliably.

A useful management convention is to identify one clear outcome owner for each activity while allowing several defined contributors. This is a design choice for clarity, not a universal CMMC requirement that every matrix contain exactly one letter A. If several approvals are genuinely necessary, explain their separate purposes and sequence rather than forcing the process into a misleading single cell.

Label	Practical meaning in this chapter	Common misunderstanding
Responsible	Performs the identified activity	Has authority to approve every related decision
Accountable	Owns completion of the defined outcome	Personally performs every technical step
Consulted	Provides needed input before the decision or action	Automatically approves the final result
Informed	Receives a defined update	Has accepted or verified the completed work

A plain-language matrix may be clearer than a RACI chart for an MSP customer with several providers. The important question is whether another qualified person can follow the responsibilities. A page filled with letters is not more mature than a page of clear assignments.

6.6 Establish the Scope and Baseline Before Assigning Rows

Chapter 5 established the assessment boundary, asset categories, information flows, and provider relationships. Use that approved scope as the starting point for Chapter 6. Without a defined environment, a responsibility matrix can become a generic list of duties that does not match any actual system.

Record the assessed organization, system name, scope version, relevant locations, and provider offerings. Identify the requirement baseline and the source version used for mapping. For Harbor Point, the matrix applies to the Engineering Collaboration System and refers to its scope record, SSP, asset inventory, and provider service descriptions. It does not silently extend every assignment to all corporate systems or every NorthStar customer.

Then examine differences within the environment. A managed engineering workstation, a hosted repository, and a specialized instrument may require different treatment. Assigning a provider responsibility for every asset in a category without checking the service boundary can overstate what the provider actually manages. Conversely, excluding an offsite security service from the matrix because it is not customer-owned can omit an important contribution.

Keep Level 1 and Level 2 distinct. A Level 1 responsibility map can be useful, but it should use the applicable Level 1 requirements and scope. It should not label every Level 2 management practice as a mandatory Level 1 obligation. Similarly, a Level 2 matrix should not be presented as complete for Level 3 without analyzing the additional applicable requirements and provider arrangements. [R1, R2]

Give the Matrix a Controlled Identity

A useful header identifies the matrix title, version, effective date, owner, related system, baseline, and approval state. A short change history records meaningful changes. The document should show whether it describes the current approved arrangement or a proposal awaiting agreement.

Harbor Point uses the identifier HP-CRM-01 for the coordinated record. NorthStar's provider CRM and Beacon's service description retain their own identifiers and versions. This arrangement allows a reviewer to see exactly which external commitments informed the customer's responsibilities. The identifiers themselves are fictional; the underlying principle is that a responsibility assignment should be traceable to a defined environment and a current source.

6.7 Inventory the People and Providers Who Must Participate

The MSP contact and the customer's senior executive are rarely the only participants needed. Responsibility mapping may require the system owner, engineering management, human resources, facilities, purchasing, contract administration, security staff, application owners, and external providers. Include people because

they perform or authorize relevant work, not merely because their titles appear in an organization chart.

At Harbor Point, human resources initiates personnel changes, but engineering management decides project access. Facilities manages keys and visitor entry. Purchasing controls which cloud offering is ordered. The system owner coordinates implementation and documentation. NorthStar operates selected technical services, while Beacon monitors the agreed sources. Each participant can expose a different missing handoff.

Represent durable roles in the matrix and maintain the current individuals and alternates in a controlled contact record. A matrix that depends on one named technician becomes inaccurate when that person changes assignments. A role without an actual staffed contact is equally weak. The two records should remain connected.

Ask each participant about limits. Does the manager have authority to approve overtime or emergency downtime? Can the technician administer the relevant application? Is the monitoring provider permitted to isolate a device? Can the evidence custodian retrieve records held by a subcontracted provider? These questions distinguish an available person from an authorized and capable participant.

Map Provider Chains Explicitly

NorthStar may purchase a monitoring service that relies on a separate platform operator. Harbor Point may contract with NorthStar rather than directly with that operator. The customer still needs to understand the relevant service dependency, the responsibilities it inherits, and the evidence access available through the arrangement.

Do not assume that the immediate provider can promise any action its downstream supplier performs. Confirm the service terms and the communication route. The customer-facing matrix can identify NorthStar as the coordinating contact while referring to the provider documentation that establishes the underlying contribution. Coordination is itself a responsibility; it should not hide uncertainty about who performs the work.

6.8 Choose a Level of Detail That Supports Action

A responsibility matrix can fail by being too broad or too fragmented. A single row for each requirement may hide multiple decisions and operators. At the other extreme, one row for every mouse click creates a maintenance burden without

clarifying the security outcome. Choose the smallest activity that has a meaningful owner, result, and handoff.

For example, create user is too narrow if the surrounding process never authorizes the user's access. Manage access is too broad if it combines new accounts, privileged roles, external identities, and termination without explaining their different triggers. Approve engineering project access and implement the approved application role are useful activities because they distinguish authority and execution.

A practical design uses linked views. A requirement view shows coverage of the applicable baseline. An activity view describes the work and handoffs. An evidence view identifies supporting records. A provider view explains inherited or supplied contributions. These can exist in one workbook or document system; they do not need to be separate files if that would create unnecessary duplication.

The same activity may support several requirements, and one requirement may depend on several activities. Preserve those relationships. Do not duplicate an identical procedure dozens of times simply to make each requirement row look independent. Use a stable activity identifier and map it to the relevant requirements and objectives.

Test Whether a Row Can Be Used

Read a proposed row to the person expected to act. Ask what starts the work, what information is required, what they are permitted to do, and how they know they are finished. If the person must invent those details, the row needs clarification or a useful procedure reference.

Harbor Point applies this test before approving the full matrix. The review turns vague statements into practical instructions while the design is still easy to change. It also avoids producing a large polished document whose apparent precision comes entirely from formatting.

6.9 Translate Requirements into Activities and Assessment Objectives

The requirement identifier tells us which security expectation we are addressing. The assessment objectives help us understand the determinations that must be supported. The activity description explains what the customer and providers do to implement and maintain that expectation. Keep all three connected, but do not treat them as interchangeable.

Consider NIST SP 800-171 Revision 2 requirement 3.1.1. The June 2018 assessment publication distinguishes identifying authorized users, processes, and devices from limiting access to those authorized populations. This distinction is valuable for responsibility mapping. A customer may identify the appropriate users while an MSP implements restrictions; application owners may identify nonhuman processes, and another technical team may control device admission. [R3, R4]

A row that simply assigns 3.1.1 to NorthStar can therefore conceal customer and application responsibilities. NorthStar can configure an access mechanism, but it needs an authoritative basis for deciding who and what is permitted. The matrix should identify that basis and the people responsible for keeping it current.

Use requirement and objective references accurately. The activity labels in this chapter are explanatory paraphrases, not replacements for the official text. When preparing a real matrix, retain the exact authoritative wording or a reliable controlled reference to it. Do not invent objective letters to make a sample look complete.

Objective grouping for 3.1.1	Activity to examine	Example contribution
Identification of authorized users	Maintain approved user population	Harbor Point identifies and approves eligible personnel
Identification of authorized processes	Register approved application identities	Application owner explains purpose and authorized use
Identification of authorized devices	Maintain approved connecting systems	Harbor Point and NorthStar reconcile authorized inventory
Access restrictions for those populations	Configure and verify enforcement	NorthStar implements the relevant technical controls

Preserve the Difference Between Mapping and Proof

A mapping shows where a responsibility belongs. It does not prove that the activity operates effectively. Harbor Point can map a device-admission task to the correct objective while still having a technical gap that allows unauthorized devices to connect. The gap must remain visible even when the ownership assignment is clear.

Similarly, a single successful test does not automatically establish every determination associated with the requirement. The evidence must support the actual claim being made. Assigning evidence preparation and verification at the activity level helps the organization avoid overstating what a screenshot or test result demonstrates.

6.10 Write a Complete Responsibility Statement

A useful responsibility statement contains an actor, an action, an object, and a condition. The actor should be a defined role or provider. The action should be observable. The object should identify the system, record, decision, or population involved. The condition should explain the trigger, timing, or prerequisite that makes the assignment meaningful.

For example, NorthStar manages accounts leaves most of the process unstated. A clearer statement is: NorthStar's identity administrator implements Harbor Point's approved project role after receiving a validated access request through the designated workflow, records the change, and routes the result for verification. This sentence describes the service without claiming that NorthStar decides the employee's business need.

The matrix can use a concise version of that statement and refer to a procedure for detailed steps. Avoid filling the main table with paragraphs so long that readers cannot compare assignments. A short activity row linked to a readable activity record is often more useful than an extremely wide spreadsheet.

Define completion in terms of the result. Account created may not mean access correctly assigned. Alert sent may not mean the alert was received and acted upon. Backup job completed may not mean protected information can be restored to an authorized destination. The completion criterion should match the outcome the process is intended to establish.

Field	What to record	Example
Activity identifier	Stable reference to the work	HP-AC-01
Requirement reference	Relevant baseline and objectives	3.1.1 with supported objective mapping
Trigger and input	What starts the activity	Validated project access request

Field	What to record	Example
Decision authority	Who approves the relevant decision	Harbor Point engineering manager
Executor	Who performs the authorized action	NorthStar identity administrator
Verification	How completion is checked	Compare implemented role with approval
Evidence and custody	What is retained and by whom	Approved request and change record in controlled repository
Exception route	What happens if the process cannot finish	Escalate to system owner without granting unapproved access

These fields are an example, not an official mandatory column set. Choose a format that remains readable and maintainable. The important feature is that the assignment can be explained without relying on an undocumented conversation.

6.11 Define Handoffs and Acceptance Criteria

Many responsibility failures occur after one party completes its own task. A customer approves access but does not identify the project. An MSP configures logging but does not tell the monitoring provider that a new source exists. A provider sends a report to an obsolete address. Each organization can point to an action; the complete process still fails.

A handoff needs a defined sender, recipient, information package, communication route, and acceptance condition. The recipient should know what to do when the input is incomplete or inconsistent. The sender should know how to determine whether the handoff was accepted. A sent email is not automatically a completed transfer of responsibility.

At Harbor Point, an access request must identify the user, project, requested role, approving authority, and relevant effective date. NorthStar validates those elements before implementation. If the request merely says copy another employee, it is returned for clarification rather than interpreted as unlimited approval. The customer retains the decision; the MSP protects the integrity of the process.

For a new log source, NorthStar supplies the source identifier, expected event types, connection details, and approved configuration. Beacon confirms receipt of representative events and reports any missing fields or interruptions. The customer system owner receives the completion status. The handoff includes an observable acceptance test, not simply a message saying logging enabled.

Design the Failure Path at the Same Time

The normal sequence is only part of the workflow. Decide what happens when the customer approver is unavailable, the provider cannot retrieve evidence, or the technical change fails. Identify an alternate contact and escalation route where appropriate. The alternate should have the necessary authority, not merely a working telephone number.

A failed handoff should leave a visible unresolved item. Do not let a task disappear because it moved from one ticket queue to another. NorthStar retains the coordinating record until the required acceptance or escalation occurs. This is a practical service design choice that helps Harbor Point understand the actual state of the work.

6.12 Work Through an Access Provisioning Record

Harbor Point needs to grant an engineer access to the controlled design repository. We will build the responsibility record from the event rather than begin with a product name. The event starts when the department identifies a business need. It ends when approved access is implemented, verified, and documented, or when the request is declined or remains unresolved.

The engineering manager identifies the appropriate project role. Human resources or another authoritative personnel process establishes the individual's employment or authorized working relationship. NorthStar verifies that the request came through the approved route and that the technical prerequisites are satisfied. These inputs serve different purposes. An employment record does not by itself authorize every project role.

NorthStar then implements the approved access in the relevant identity and application systems. The technician records the actual groups, roles, or permissions changed. A designated reviewer compares those changes with the approval and checks the relevant access behavior. Where the review identifies an error, the task remains open until the discrepancy is corrected and verified.

The evidence package contains the authorization, the implementation record, and the verification result. It should identify the user and system clearly enough to connect the records without exposing unnecessary sensitive information. The customer controls who may retrieve the package, while the MSP contributes the records it produces under the service arrangement.

Sample Activity Record HP-AC-01

Purpose: establish authorized project access for an identified person. Scope: the Engineering Collaboration System and its designated identity and repository services. Requirement relationships: selected access-control and identification responsibilities, mapped to the applicable objectives during implementation review.

Decision: Harbor Point's engineering manager approves the specific project role. Execution: NorthStar's identity administrator implements that role after validating the request. Verification: the designated access reviewer checks the implemented permission and the relevant allowed and denied behavior. Evidence: the approved request, change details, and verification record are retained through the controlled evidence process.

Failure handling: an incomplete request is returned to the requestor; a conflicting approval is escalated to the system owner; an implementation failure remains an open service task. NorthStar does not expand permissions merely to make an application error disappear. Any proposed broader access requires a separate authorized decision.

This example is intentionally more specific than customer owns access and MSP manages accounts. It identifies the customer's business decision, the provider's technical action, and the evidence linking them. The same structure can be adapted to another application without assuming that its permission model is identical.

6.13 Map Personnel Changes and Access Removal

The access process must respond when a person changes duties or leaves. A matrix focused only on onboarding will miss some of the most consequential handoffs. The customer often has the earliest knowledge of a personnel event, while the provider has the ability to change accounts and devices. The process depends on timely, authorized communication between them.

Harbor Point's personnel function identifies the change and initiates the approved notification. The manager identifies project access that should end or change. NorthStar performs the technical actions within its service scope. Application owners

address permissions not administered by NorthStar. Facilities handles relevant physical access. A coordinating role checks that the required actions across these systems have been addressed.

The matrix should distinguish disabling an account from revoking all relevant access. Existing sessions, external application permissions, privileged roles, remote access, device possession, and shared secrets may need separate consideration. Not every environment has the same mechanisms, so the procedure should follow the actual architecture rather than copy a universal checklist without review.

For an application identity owned by a departing employee, the decision may be to transfer ownership, rotate credentials, modify permissions, or retire the integration. Simply disabling the employee's account may leave that process running. Assign someone who understands the application dependency and has authority to decide its continuing business purpose.

Handle Urgent Events Without Improvised Authority

An urgent termination may require coordinated timing and limited distribution of personnel information. Establish the authorized instruction route in advance. NorthStar needs enough information to perform the technical work, but a broad service ticket does not need to contain the full employment dispute.

The completion record should show which systems were addressed, which actions succeeded, which remain unresolved, and who owns follow-up. A closed umbrella ticket with no supporting detail can hide a missed application. The coordinator verifies the complete event, while each operator remains responsible for the accuracy of its own action record.

6.14 Assign Privileged Access and Authentication Responsibilities

Privileged access requires more than naming the administrator. The organization must identify the authorized administrative functions, the people permitted to perform them, the mechanisms used, and the oversight that applies. An MSP may need broad technical capability to support the environment, but that does not justify treating every technician or support tool as automatically authorized.

Harbor Point approves the service roles and permitted administrative activities. NorthStar manages its assigned personnel and access according to the agreed arrangement. The implementation must address the actual customer environment and relevant provider systems. A generic statement that all technicians follow company

policy does not explain which technicians can administer Harbor Point's repository or how that access is removed.

Authentication responsibilities also cross boundaries. A platform may provide a multifactor authentication capability. NorthStar may configure the relevant policy. Harbor Point may identify the authorized user population and enforce enrollment. Support staff may manage recovery under a controlled process. A subscription that includes the feature does not prove that the feature is applied to every required access path. [R3, R4]

Use the applicable requirement text when defining coverage. For example, the Revision 2 multifactor authentication requirement distinguishes privileged and nonprivileged access conditions. Do not reduce it to the vague statement everyone has MFA without checking the covered paths and actual implementation. The matrix should identify who evaluates those paths and who maintains the configuration.

Recovery Is Part of the Responsibility Design

A user who loses an authenticator still needs an authorized recovery process. Assign who verifies identity, who approves any exceptional action, who performs the reset, and what evidence is retained. A support technician should not be left to decide identity assurance from familiarity with a caller's voice.

Administrative emergency access deserves the same clarity. Define the circumstances, authority, safeguards, and subsequent review for its use. The purpose of an emergency mechanism is to maintain an authorized recovery capability, not to create an undocumented bypass. Include responsibility for testing that the mechanism remains usable under the conditions for which it was designed.

6.15 Divide Logging Responsibilities Across the Entire Pipeline

Logging is a useful example because one word conceals several different activities. Someone must identify the events needed, define useful record content, configure generation, transport the records, retain them, protect them, and review relevant activity. A provider may perform only part of that chain.

NIST SP 800-171A's assessment objectives for 3.3.1 distinguish the specification of events and content from record generation and retention. This gives the matrix a practical structure. Harbor Point's security function determines the information needed for its environment with technical input from NorthStar and Beacon.

NorthStar configures sources it manages. Beacon receives and analyzes the agreed records under its service description. [R4]

The parties should verify that the records arriving at the monitoring service contain the intended fields. A successful connection can still produce incomplete data. For example, a source may send event names without a usable user identifier, or a connector may omit the relevant application activity. The matrix should identify who discovers and resolves those discrepancies.

Retention is another separate decision. Harbor Point identifies its applicable obligations and approved retention needs. The providers explain available capabilities, costs, and limits. The selected configuration must support the decision. A platform default should not silently become the customer's retention policy merely because nobody assigned responsibility for evaluating it.

Activity	Example lead	Required handoff
Identify needed events and content	Harbor Point security owner	Obtain technical feasibility input from providers
Configure managed log sources	NorthStar	Supply source details and sample records to Beacon
Confirm collection and useful fields	Beacon with NorthStar	Report accepted sources and unresolved defects
Configure agreed retention	Relevant platform administrator	Demonstrate settings and retrieval behavior
Review and escalate relevant activity	Beacon under its agreed service	Route findings to designated customer and MSP contacts
Address source or collection failures	Assigned technical owner	Confirm restored collection to the monitoring function

Do Not Confuse Three Different Retention Duties

Operational log retention, preservation of records related to an incident, and retention of assessment artifacts are related but distinct. Their triggers, content, and time periods can differ. The matrix should identify the applicable source and owner for each rather than placing every record under one arbitrary number.

For Level 2 certification assessments, the published CMMC rule requires the organization to retain the hashed artifacts used as assessment evidence for six years from the CMMC Status Date and describes the associated integrity records. This does not mean that every operational log must automatically be retained for six years under that provision. Incident preservation under an applicable contract clause is another separate obligation. [R2, R6]

6.16 Connect Monitoring to an Authorized Response

Monitoring provides value when relevant findings reach someone who can act. The matrix should describe what the service monitors, what kinds of activity it analyzes, how findings are communicated, and what response duties are included. A phrase such as continuous monitoring can otherwise create expectations that the service agreement does not support.

Beacon's fictional service identifies the agreed sources and provides analysis and escalation. Harbor Point and NorthStar must decide whether Beacon may take any direct containment action, whether NorthStar may isolate a device under predefined conditions, and when customer authorization is required. These decisions should reflect the actual service capability and business impact.

Separate detection, triage, containment, investigation, recovery, and reporting. One organization may perform several of these activities, but they are not the same task. A service that opens an alert ticket should not be described as completing incident response unless its agreement and operating practice support that claim.

The response route should also distinguish ordinary business hours from other periods when the customer relies on the service. If a provider is available continuously but the customer decision-maker is unavailable overnight, the overall process may still have a coverage gap. Assign an authorized alternate or define an appropriate action within the agreed conditions.

Test the Communication Route

Use a controlled exercise to confirm that a representative notification reaches the current contacts and receives the expected response. Record what happened. If the message reaches a mailbox nobody monitors, changing its priority label will not resolve the problem. The responsibility allocation needs a functioning recipient and escalation path.

At Harbor Point, the first exercise reveals that Beacon's escalation list still names a former NorthStar technician. The service exists and the alert is generated, but the handoff is ineffective. Updating the contact record, confirming receipt, and testing the alternate route addresses the actual failure. The matrix then identifies who maintains that contact record when staffing changes.

6.17 Build Incident Responsibilities Before an Incident Occurs

An incident creates pressure to act quickly while facts remain incomplete. This is a poor time to decide who may disconnect a production system, communicate with the customer, preserve evidence, or make a required external report. The responsibility matrix should connect to an incident response plan that establishes those authorities and procedures in advance.

Harbor Point names an internal incident decision-maker and alternates. NorthStar performs the technical response actions authorized by the arrangement. Beacon supplies relevant monitoring information and analysis. Other specialists may assist under a defined engagement. Contract administration and qualified advisers help determine applicable reporting obligations. The matrix should show the route without pretending that one technician supplies every business and legal decision.

NIST SP 800-171 Revision 2 includes incident handling, tracking and reporting, and testing responsibilities. A practical matrix should identify the people who maintain the capability, conduct exercises, act during an event, and document the results. A written response plan is an input to that capability; it is not evidence that every participant can execute it. [R3]

When DFARS 252.204-7012 applies, its reporting and preservation provisions must be addressed on their own terms. The clause defines rapid reporting in relation to discovery and includes a 72-hour reporting period. It also requires specified media and monitoring data to be preserved for at least 90 days from submission of the incident report. The customer must verify applicability and implement a process capable of meeting the actual obligations. An MSP's routine ticket response target does not replace them. [R6]

Keep Provider Notification and Government Reporting Separate

A provider notifying Harbor Point does not by itself establish that a required report has reached the government or another required recipient. Assign who evaluates the reporting trigger, who prepares supporting facts, who has the required submission

authority and access, and who retains the confirmation. Prepare these capabilities before an incident creates a deadline.

Likewise, a customer report does not automatically satisfy every provider or subcontractor duty. Identify the obligations associated with each applicable agreement and clause. The purpose of the matrix is to connect the work and evidence without obscuring the separate responsibilities of the parties.

6.18 Assign Vulnerability and Remediation Work Separately

A vulnerability report identifies a condition that needs evaluation. It does not determine every operational decision required to address that condition. The matrix should distinguish inventory coverage, scanning, interpretation, prioritization, change approval, remediation, verification, and tracking of unresolved findings.

NorthStar may operate the scanning capability for managed assets. Harbor Point's application owner understands whether a proposed change could interrupt an engineering workflow. The security owner evaluates the exposure and proposed treatment. A technician implements an authorized correction. A verification activity checks whether the relevant condition has been resolved. Each step contributes something different.

Do not assign the entire process to the provider that supplies the report unless that provider actually has the authority and capability to perform all of the work. A scanner cannot approve downtime, replace an unsupported business application, or decide whether a proposed exception is acceptable to the customer. Those decisions need identified owners and a record of their basis.

When remediation cannot occur immediately, record the condition, affected assets, reason, interim measures, decision authority, next action, and review trigger. Avoid treating a manager's acceptance as proof that the security requirement is met. An operational risk decision and a formal CMMC assessment result are different matters. Whether a particular deficiency can be addressed through a permitted assessment POA&M depends on the applicable CMMC rules, not the color of an internal task tracker.

Verify the Result in Context

A completed patch deployment task does not necessarily prove that every intended device received the update. Some devices may have been offline, a restart may be

pending, or a component may have failed. The matrix should identify who compares the intended population with actual results and who follows up on exceptions.

Harbor Point uses the asset inventory to define the managed population, NorthStar supplies deployment results, and the relevant technical owner verifies the remaining exposure. If a specialized instrument cannot accept the same change as an ordinary workstation, the team evaluates its actual category and treatment. It does not conceal the difference by marking the entire fleet complete.

6.19 Connect Configuration Changes to Approved Baselines

Configuration management involves deciding what the approved state should be and controlling changes to that state. An MSP may maintain technical settings, but the customer needs a way to understand significant changes, approve relevant business impacts, and preserve the intended protection of the assessed environment.

Harbor Point's system owner coordinates the approved configuration baseline. NorthStar proposes and implements changes for systems within its service scope. Application owners review compatibility and operational effects. The designated security reviewer evaluates relevant security impacts. The precise approval path depends on the change; not every routine update requires the same meeting as a major architectural change.

The matrix should identify who maintains the baseline record, who can propose a change, who approves it, who executes it, and who verifies the result. It should also identify how a change updates the SSP, inventory, diagrams, responsibility assignments, or provider records when those documents are affected. A technically successful change can still leave the documentation inaccurate.

Consider enabling an export function in the engineering repository. The request may appear to be a usability improvement. It may also create a new information flow, require a new destination, or change which assets handle CUI. The technical operator should route the proposal for the relevant scope and security review before implementation, rather than treat the feature as an isolated application setting.

Define Emergency Change Review

An emergency may require an accelerated approval route. Identify who can authorize it, what minimum information must be recorded, and what review follows. The record should preserve the reason, scope, actions, and observed outcome. An emergency label should not erase the evidence of what changed.

After the immediate condition is stabilized, the appropriate owners reconcile the baseline and related records. If the temporary configuration creates an ongoing dependency or responsibility, the matrix must reflect it. The emergency process is complete only when the lasting state is understood and managed.

6.20 Address System Integrity and Protective Tools as Services

Protective software requires deployment, configuration, monitoring, updating, and response to failures. A matrix that names the endpoint protection product without assigning those activities describes a purchase rather than an operating service. The customer needs to know which devices are covered and what happens when coverage changes.

NorthStar maintains the agreed agents and configuration on managed engineering endpoints. Harbor Point supplies information about newly acquired systems and approved exceptions. Beacon may receive relevant detections under its monitoring arrangement. Each party needs a reliable way to identify missing agents, disabled features, outdated components, or endpoints that have stopped reporting.

NIST SP 800-171 Revision 2 includes system and information integrity requirements addressing flaws, malicious code, security alerts, monitoring, and related protections. Map the actual service contributions to the applicable requirements and objectives. Do not assume that a product's marketing label proves that every relevant requirement is fully addressed. [R3, R4]

The matrix should identify who maintains the approved policy, who can authorize an exception, who implements it, and who reviews its continuing need. If an engineer reports that a protective setting interferes with an application, the support process should investigate the issue and evaluate a specific authorized change. Disabling the protection indefinitely to close the ticket would create a different outcome from the one the customer intended.

Assign the Work Created by a Detection

A detection may require more than acknowledging the alert. Someone may need to determine whether the activity is expected, preserve relevant information, contain an affected device, correct the cause, and verify recovery. The protective tool's activity connects to the monitoring and incident responsibilities discussed earlier.

Harbor Point's matrix uses references between these activities instead of duplicating the entire response plan in every product row. A technician can see where a tool event

enters the response process and which authority applies. This is especially useful when several tools detect the same event and the customer needs one coordinated response.

6.21 Divide Backup and Recovery Responsibilities Across the Workflow

Backup is often described as a fully managed service. That phrase still leaves questions about the protected information, retention decisions, encryption, credential management, failed jobs, restoration authority, and recovery verification. The responsibility matrix should describe the workflow the customer actually relies upon.

Harbor Point identifies the information and business processes that require protection and recovery. NorthStar configures the agreed backup service for the approved sources. The provider supplies the capabilities described for the selected offering. The customer and MSP establish who investigates failures, who authorizes a restoration, and who verifies that recovered information is placed in an approved destination.

A backup operator may be capable of restoring data into several environments. The ability to restore does not establish that every destination is authorized to receive the information. The matrix should connect restoration approval to the scope and information-handling decisions from Chapter 5. A recovery action can otherwise create a new uncontrolled copy while appearing to be a routine support task.

Recovery objectives, service commitments, and test schedules should be established for the actual business need and applicable obligations. Do not present a fictional test interval as a universal CMMC mandate. The relevant requirements must be mapped accurately; broader business continuity objectives may also justify tasks that extend beyond a single CMMC requirement.

Verify Recovery Through the People Who Depend on It

NorthStar can confirm that a restoration job completed, but Harbor Point may need to confirm that the recovered files are usable and appropriate for the intended work. Assign the business validation as well as the technical validation. A readable archive of the wrong project is not a successful recovery outcome.

Retain a record of the authorized request, selected recovery point, destination, technical result, and business validation where applicable. If a test fails, assign

corrective work and a follow-up verification. The failed test is useful information; it should not be replaced by a later success record that conceals what was learned.

6.22 Include Awareness and Role Training in the Matrix

An MSP can supply training material or a learning platform without controlling whether the right people receive training, understand local procedures, or complete required follow-up. The responsibility matrix should separate content delivery from the customer's personnel and management responsibilities.

Harbor Point identifies the relevant workforce and the roles that need additional instruction. NorthStar may help explain the approved technical workflow and provide service-specific material. The training coordinator assigns the appropriate content, tracks completion, and routes overdue or incomplete work to the responsible manager. The customer confirms that the instruction reflects its actual systems and information-handling practices.

NIST SP 800-171 Revision 2 distinguishes general awareness, role-related training, and awareness of potential insider threat indicators. A single generic course may contribute to these activities, but its existence does not prove that all relevant instruction has occurred. Map the actual content and participant population to the applicable requirements. [R3]

The matrix should also address changes. An employee who becomes an administrator may need different instruction from an ordinary user. A new remote-work method may require updated guidance. A changed incident reporting route may invalidate an old training slide. Assign who recognizes these triggers and who updates the material.

Make Completion Records Meaningful

A training record should connect the participant, content or course version, date, and relevant result. Where the organization uses an acknowledgment or exercise, retain the record according to its approved process. Avoid collecting unnecessary personal information merely to make the evidence package appear substantial.

Harbor Point's managers are responsible for resolving noncompletion within their teams. NorthStar can provide reports and technical support, but it cannot quietly become the employer's disciplinary authority. The matrix helps both parties understand the limits of the service and the actions the customer must take.

6.23 Assign Personnel and Physical Protection Duties Explicitly

Personnel security and physical protection are frequently underrepresented in an MSP's first matrix because the initial discussion begins with technology. These areas involve customer decisions, facilities, and human processes that the MSP may not operate. The duties should remain visible even when the service agreement excludes them.

Harbor Point's personnel function manages the applicable screening and personnel-change processes. Facilities controls the relevant physical access mechanisms and visitor practices. Managers supervise authorized work. NorthStar may administer an electronic access system or provide technical records, but that service does not automatically include escorting visitors, collecting keys, or deciding personnel suitability.

A landlord or shared-office operator may provide building entry controls. Harbor Point still needs to determine which spaces, devices, media, and activities depend on those controls and which protections it must perform itself. A building badge system does not explain what happens when a visitor enters the engineering work area or when printed material is left unattended.

The matrix should identify the actual locations and conditions. Corporate office procedures may not fully describe a remote employee's authorized workspace. Conversely, a remote-work assignment should not imply that the MSP controls the employee's entire household. Define the relevant responsibilities and verify that the approved work arrangement supports them.

Follow a Visitor Event

A service technician arrives to maintain equipment. The customer identifies who authorizes the visit, verifies the person's access, provides any required supervision, protects information in the work area, and records the event. NorthStar coordinates its own technician if that falls within the service arrangement. The customer remains responsible for the facility activities it operates.

Walking through this event often reveals a gap that a high-level physical security row misses. Someone may control the door while nobody is responsible for the visitor after entry. Assign the complete activity, including the departure and return of temporary access where relevant. The matrix should reflect the actual procedure the customer can perform.

6.24 Map Media Handling and Authorized Information Exchange

Information moves through files, removable media, printed pages, collaboration services, support exchanges, and disposal processes. The responsibility matrix should identify who authorizes those movements, who implements the approved restrictions, and who verifies the handling of the information at each stage.

Harbor Point's information owner identifies the authorized business purpose and recipients. NorthStar configures the designated transfer mechanisms and restrictions within its service scope. Users follow the approved workflow. The relevant owner addresses exceptions, such as a partner requesting a transfer method the customer has not approved. The technician should not decide the recipient's need to know simply because the transfer is technically possible.

For disposal, distinguish deciding that information or equipment may be retired from performing the approved sanitization or destruction process. Someone must identify the assets and applicable handling requirements, authorize the action, select an appropriate method, perform or arrange the work, and retain supporting records. A disposal vendor's certificate can contribute evidence, but the customer still needs to connect it to the actual assets and authorized process.

Printed information creates similar duties. If printing is permitted, identify who controls the output, storage, access, transportation, and disposition. If printing is prohibited in a particular workflow, assign who maintains the restriction and handles business requests that conflict with it. The matrix should not assume that a policy sentence makes the technical and human activities unnecessary.

Keep Support Evidence Within the Approved Flow

A screenshot or diagnostic archive may contain information that changes how a support exchange must be handled. NorthStar's technicians need a defined route for reviewing and transferring such material. Harbor Point must know which support services are authorized to receive it and how the related provider responsibilities are documented.

The same principle applies to assessment evidence. Do not export sensitive configurations, user lists, or project information into an ordinary shared folder merely because the file is now called evidence. Assign a custodian and an approved exchange method based on the content and purpose of the records.

6.25 Address Maintenance and External Technical Support

Maintenance can introduce people, tools, software, remote connections, and diagnostic media into the assessed environment. The responsibility matrix should describe how the customer authorizes maintenance and how the provider performs it within the relevant restrictions. A vendor's need to repair a system does not automatically authorize every support technique.

Harbor Point identifies the maintenance need and business constraints. NorthStar coordinates activities within its service scope. A specialized application vendor may perform separate work under a defined arrangement. The matrix should identify who approves the connection or visit, who verifies the provider's identity and permitted activity, who supervises where appropriate, and who confirms that temporary access ends.

Technical support can also create new data flows. A vendor may request logs, a memory dump, or a copy of an application database. The responsible parties must evaluate the content and destination before transfer. A routine support ticket is not a substitute for the scope and information-handling decision.

Where tools or media are introduced, assign the relevant inspection, approval, and handling tasks according to the applicable requirements and procedures. The details depend on the environment. The matrix should link to the procedure that defines them rather than imply that the same generic remote session covers every maintenance scenario.

Close the Maintenance Event

Completion includes more than the system working again. The responsible parties should address temporary accounts, changed settings, transferred information, introduced tools, and any documentation that needs updating. Record unresolved actions rather than assume that the vendor completed everything before disconnecting.

At Harbor Point, a vendor resolves an application error by enabling an additional service. The repair succeeds, but the new service changes the approved configuration. NorthStar identifies the change during the closing review and routes it for the appropriate evaluation. The matrix makes that review part of the maintenance event instead of relying on someone noticing later.

6.26 Assign Risk Assessment and Security Assessment Responsibilities

A customer can buy technical assessment services while still retaining important decisions about business impact, risk treatment, and implementation priorities. The matrix should identify who gathers facts, who analyzes them, who supplies operational context, who approves the response, and who tracks the resulting work.

NorthStar may provide inventory, vulnerability information, configuration observations, and technical recommendations. Harbor Point supplies business priorities, contract context, information-handling needs, and the consequences of operational disruption. The security owner coordinates the analysis. The designated management authority decides among permissible treatment options with an understanding of the applicable requirements.

The same distinction applies to a security assessment. A consultant or MSP can review implementation and identify gaps. That internal readiness activity should not be described as a CMMC certification assessment unless it is conducted through the required authorized process. The matrix should identify the role accurately and avoid suggesting that a service provider can guarantee the customer's certification outcome. [R2]

NIST SP 800-171 Revision 2 addresses risk assessment, security assessment, plans of action, monitoring, and SSP maintenance in its relevant requirement families. The matrix should connect these activities without collapsing them into a single annual compliance review. Each has a purpose and may be triggered by different conditions. [R3]

Preserve the Decision and Its Basis

When Harbor Point prioritizes a corrective action, the record should explain the affected condition, proposed response, owner, resources, and next review. A provider's recommendation is an input to that decision. A management signature should not erase the underlying technical facts or transform an unmet requirement into a met one.

The next chapter will examine the gap assessment in greater depth. The responsibility work in this chapter prepares for that process by identifying the people who can explain implementation, supply evidence, validate findings, and carry out corrections. Without those assignments, a gap assessment may produce a useful report that nobody is positioned to act upon.

6.27 Analyze Cloud Responsibilities at the Offering Level

A cloud provider's responsibilities depend on the selected service and configuration. The customer should identify the exact offering, relevant boundary, enabled features, and provider documentation. A statement that a major vendor is compliant does not establish what Harbor Point may rely upon in its own implementation.

A provider may secure the underlying infrastructure while Harbor Point remains responsible for its users, information, tenant settings, endpoint access, and integration choices. NorthStar may perform some customer-side administration under its agreement. The coordinated matrix should show these contributions separately so that the provider's responsibility is not mistaken for completion of the customer's task.

For a CUI-handling cloud offering used in the published Level 2 certification framework, the rule addresses FedRAMP authorization at the appropriate baseline or equivalent security requirements under DoD policy. The scoping provisions also connect relevant CRM responsibilities to the customer's SSP. This is a service-specific analysis; a provider-wide claim is insufficient. [R1, R2]

Do not assume that a cloud security control transfers unchanged to every customer asset. A physical protection implemented in a provider's data center does not secure a printed drawing in Harbor Point's office. A platform authentication capability does not establish the customer's approved user population. The matrix should identify the layer and condition under which the provider contribution applies.

Read Customer Responsibilities as Required Work

When the provider says the customer must configure a setting or enable a feature, assign that action to a capable operator and identify verification. If NorthStar will perform it, confirm that the service agreement includes it. If Harbor Point retains it, identify the internal role and required access.

Keep the provider document version associated with the matrix. An updated service, changed feature, or revised responsibility statement may affect the customer's implementation. Assign someone to review relevant provider changes and determine whether the coordinated matrix, SSP, or technical configuration needs updating. Downloading a CRM once is not a complete management process.

6.28 Substantiate Inherited and Shared Contributions

Inherited is a useful word only when the customer can explain what is inherited, from whom, for which service, and under what conditions. It should not function as a shortcut that removes a requirement from discussion. A provider contribution may satisfy part of an implementation while leaving important customer actions necessary.

NorthStar records the requirement relationship, the provider offering, the specific contribution, the customer prerequisites, and the supporting evidence or assurance source. Harbor Point records how its environment uses that contribution. The result should allow a reviewer to follow the reasoning from the customer's implementation to the provider capability without assuming that an entire requirement family is automatically complete.

For example, the cloud provider may operate a logging capability. Harbor Point and NorthStar may still need to identify relevant events, enable appropriate collection, configure retention, review activity, and respond to findings. If the customer has not enabled the required feature, the provider's available capability does not become an implemented customer control merely through the word inherited.

Shared should be decomposed in the same way. Identify the customer's task and the provider's task, then describe the handoff. If both parties must act, record both contributions. If neither party has accepted a necessary task, classify it as an unresolved assignment rather than conceal the gap behind a shared label.

Proposed statement	Question it leaves unanswered	Better description
Access is inherited from the cloud	Who authorizes users and configures roles?	Identify platform capability and customer-side access tasks
Logging is shared	Who enables sources and checks collection?	Assign source configuration, acceptance, retention, and review
Physical security is provider-owned	Which location and which assets?	Limit the claim to the provider boundary and identify local duties
MSP handles compliance	Which implementation and evidence activities?	Describe specific services and retained customer decisions

Make Evidence Access Part of the Arrangement

A provider may protect proprietary information or other customers' records. Resolve an appropriate evidence route in advance, such as an authorized document package, scoped demonstration, or coordinated assessment access. Do not assume that customer personnel are entitled to unrestricted access to the provider's entire environment.

At the same time, confidentiality concerns do not prove that a contribution is effective. If the required support cannot be obtained through an acceptable route, identify the limitation and resolve it before relying on the claim. An unresolved evidence dependency is a real readiness issue, even when the service operates well in ordinary use.

6.29 Design Evidence Responsibilities Before Collection Begins

Evidence becomes difficult to manage when nobody has decided what will be produced, who may access it, or where it will remain available. The matrix should identify evidence responsibilities while the operating process is being designed. Waiting until the assessment is scheduled can reveal that important records were never generated or have already expired.

Separate the producer from the custodian and the reviewer. NorthStar may produce a configuration export. Harbor Point may retain the assessment copy in its controlled repository. A security reviewer may evaluate whether the export supports the implementation claim. These roles can overlap, but the responsibilities should be explicit.

Identify the record's purpose. An authorization supports the decision to grant access. A configuration record supports how access is implemented. A test result supports observed behavior under defined conditions. One artifact may support several claims, but its relevance should be explained. A large folder of screenshots is not automatically a coherent evidence package.

Use stable evidence identifiers and include enough context to interpret the record: system, source, date or period, relevant configuration, and associated activity. Maintain the appropriate access restrictions. Avoid collecting complete customer data when a narrower authorized record would answer the question. The objective is sufficient, reliable evidence, not maximum volume.

Preserve Assessment Artifacts Through the Required Period

For a Level 2 certification assessment, the rule's artifact-retention and integrity provisions apply to the hashed artifacts used as assessment evidence. Harbor Point should identify who preserves the files, who maintains the associated names and hash information, and how authorized retrieval will work over the required period. Delegating storage to a provider does not remove the organization's obligation. [R2]

The service agreement should address what happens if Harbor Point changes providers, an account is closed, or a platform is retired. If the only copy remains in a temporary provider portal, the retention plan may depend on access that disappears at contract termination. Plan the authorized preservation or transfer before that event occurs.

6.30 Reconcile the Matrix with Service Agreements and Resources

A matrix is not operationally credible when it assigns work that nobody has agreed to fund, staff, or perform. Compare the proposed responsibilities with the actual service descriptions and agreements. Look for tasks that fall between a base subscription, a project engagement, and an optional service.

NorthStar's standard offering may include operating-system updates but exclude a specialized engineering application. Beacon may analyze alerts but exclude direct containment. A cloud provider may retain certain records only when a particular feature or service tier is enabled. The matrix should reflect these facts and make remaining customer responsibilities visible.

If the customer needs a task that the current service does not include, identify the options and the decision owner. Harbor Point may purchase additional service, assign a qualified internal resource, use another provider, or change the design. It should not mark the task complete because a future purchase is expected. Nor should NorthStar silently absorb an undefined obligation and assume the customer understands the cost and authority involved.

Record dependencies on customer inputs. An MSP may need an approved user list, application maintenance window, or business decision before it can act. The agreement and workflow should identify the required input and what happens when it is late or incomplete. This protects the process from becoming a dispute about which party was waiting for the other.

Make the Promised Capacity Plausible

Ask whether the assigned role has the necessary skills, access, tools, and availability. A single employee may be named as owner for many activities, but the workload may exceed what that person can realistically perform. A provider may offer a capability that requires a configuration or license the customer has not purchased.

Responsibility mapping can therefore inform budgeting and staffing. It shows the work needed to sustain the environment and the assumptions behind the service price. The discussion should remain factual: which task is required, who will perform it, and what resources make that assignment credible.

6.31 Track Assignment Status Separately from Implementation Status

A common mistake is using one green status cell to mean several different things. It may mean an owner has been named, the service has been purchased, the configuration has been deployed, evidence has been collected, or an assessor has found the requirement met. Those are different states and should not be combined.

Harbor Point tracks assignment status separately from implementation and verification. An activity can have an agreed owner while the technical implementation remains incomplete. A configuration can exist while evidence access is unresolved. A reviewed internal record can support readiness without representing a formal assessment finding.

Useful assignment states include proposed, agreed, and unresolved. Implementation states should describe actual conditions in the organization's chosen tracking system. Verification should identify what was checked and when. Avoid inventing official CMMC statuses for internal workflow convenience; use labels that are clearly internal management terms.

Situation	What the matrix can honestly say	What it should not imply
Provider accepts a future task	Assignment agreed and work planned	Requirement already implemented
Technical configuration deployed	Implementation completed pending verification	Every relevant objective has been demonstrated
Evidence unavailable	Evidence dependency unresolved	Provider claim is automatically sufficient

Situation	What the matrix can honestly say	What it should not imply
Internal walkthrough succeeds	Defined workflow verified under stated conditions	Certification guaranteed
Customer accepts an operational risk	Decision recorded with its basis	Unmet CMMC requirement waived

Escalate Unresolved Assignments as Decisions

An unresolved row should identify the missing decision, responsible decision-maker, next action, and target for resolution. Do not leave it as an empty cell that a reader may mistake for not applicable. If the task is genuinely inapplicable, record the basis and have the appropriate person review it against the actual requirement and scope.

The matrix is useful precisely because it makes missing work visible. A document in which every row appears complete through vague labels is less useful than one that clearly identifies the few decisions preventing readiness.

6.32 Build the Harbor Point Matrix from Discovery to Approval

We will now combine the method in a single engagement. Harbor Point has completed an initial scope package for its Engineering Collaboration System. It relies on NorthStar for selected technical administration, Beacon for monitoring, and an identified cloud offering for the repository and supporting capabilities. Management asks NorthStar to prepare the responsibility matrix before the gap assessment begins.

NorthStar's first draft uses its standard service catalog. Most technical requirements are assigned to NorthStar, physical protection is assigned to Harbor Point, and cloud-related requirements are marked inherited. The document looks organized, but its categories are too broad. It reflects how the services are sold more closely than how the work must occur.

Step One Confirm the Actual Service Boundary

The team reviews the scope, inventory, data flows, and provider descriptions. It discovers that the engineering application has its own role assignments, which NorthStar's base service does not administer. The cloud backup order also excludes a retention feature assumed by the recovery plan. Both issues require decisions before the matrix can describe the intended implementation accurately.

Harbor Point assigns application access administration to a qualified internal application owner, with NorthStar supporting the related identity service. Purchasing resolves the backup offering and confirms the enabled feature with the provider. The matrix records the actual arrangement after these decisions rather than retaining assumptions from the first proposal.

Step Two Separate the Business Decisions

The access workshop reveals that managers have been sending requests that say give this person engineering access. The team defines project roles and the authority to approve them. Human resources confirms personnel status through a separate process. NorthStar agrees to validate the request before configuring its part of the access chain.

The matrix now distinguishes personnel information, project authorization, identity configuration, application role assignment, and verification. It does not assign all of these activities to the same party merely because they relate to one account. Each role can explain its contribution and the input it needs.

Step Three Define the Monitoring Handoff

Beacon's service description covers selected sources and analysis, but Harbor Point assumes every new cloud feature is automatically monitored. NorthStar identifies which source configuration tasks it performs. Beacon identifies the information needed to accept a new source. The customer system owner is assigned to review the coverage when applications or integrations change.

The team also resolves containment authority. Beacon will provide the agreed analysis and escalation. NorthStar may perform specifically authorized technical containment actions under the incident procedure. Harbor Point retains the defined business decisions and external reporting responsibilities. The procedure identifies alternates and a route for urgent decisions.

Step Four Establish the Evidence Route

NorthStar's standard ticket portal retains operational records under its service policy, while Harbor Point needs controlled assessment artifacts to remain available through the applicable retention period. The parties agree how relevant records will be identified, exported or preserved, protected, and retrieved. Beacon provides an authorized route for relevant service evidence without exposing other customers' information.

The matrix assigns evidence production to the party generating the record and overall assessment-artifact custody to Harbor Point's designated custodian. The record also identifies the providers' continuing contribution where needed. This prevents evidence ownership from being confused with unrestricted access to a provider's environment.

Coordinated Matrix Extract

The following extract summarizes selected activities after the workshop. It is not the complete baseline mapping. Each row links to a fuller activity record, relevant requirements and objectives, the applicable procedure, and the supporting evidence plan.

Activity	Harbor Point contribution	Provider contribution
Project access authorization	Engineering manager approves person and role	NorthStar validates the request before identity changes
Application role assignment	Application owner implements approved local role	NorthStar supports the connected identity configuration
Personnel access removal	Personnel function initiates change and owners identify affected access	NorthStar removes managed access and supplies results
New monitoring source	System owner approves required coverage and data handling	NorthStar configures source and Beacon verifies collection
Alert response	Incident decision-maker supplies defined authority and business context	Beacon analyzes and escalates; NorthStar performs authorized response
Configuration change	Relevant owner approves business and security decisions	NorthStar implements managed changes and records results

Activity	Harbor Point contribution	Provider contribution
Approved restoration	Data owner approves information and destination	NorthStar performs restoration and supports verification
Assessment evidence	Custodian controls retained assessment package	Providers produce and make agreed supporting records available
Physical entry	Facilities performs local authorization and visitor control	Provider personnel follow approved access procedure
Provider change	System owner reviews scope and responsibility impact	NorthStar coordinates technical transition and service evidence

Step Five Validate the Proposed Arrangement

The team chooses a new-user request, an urgent personnel change, a missing log source, a failed backup, and an after-hours alert. Participants walk through each event using the proposed matrix and procedures. They use representative test records and authorized demonstrations where appropriate.

The access walkthrough succeeds until the application owner is unavailable. The matrix names the primary role but no alternate. The monitoring test reveals that the source acceptance message reaches NorthStar but not Harbor Point's system owner. The backup walkthrough reveals that business validation of restored files has no assigned participant. These are specific process gaps, not reasons to abandon the entire matrix.

Harbor Point assigns a trained application alternate, corrects the notification route, and identifies an engineering reviewer for recovery validation. The team repeats the affected portions to confirm that the changes resolve the observed problems. It does not repeat unrelated tests simply to make the review appear more extensive.

Step Six Approve and Operate the Record

The appropriate customer and provider representatives confirm the assignments within their authority. The matrix is issued with a version and effective date. The SSP

and provider records are reconciled. Outstanding implementation gaps remain in the readiness tracker with owners and next actions; approval of the matrix does not conceal them.

A month later, Harbor Point enables a new collaboration feature. The change process identifies a new data flow and new application permissions. Because the matrix has an owner and a review trigger, the responsibility analysis occurs before the new workflow becomes routine. The document is now part of operating the environment rather than an artifact prepared only for an assessor.

6.33 Validate the Matrix Through Examination Interview and Testing

NIST SP 800-171A describes assessment methods that include examination, interview, and testing. These methods also provide a useful way to evaluate a responsibility design during readiness work. The internal activity should remain clearly distinguished from the formal CMMC assessment process and its required procedures. [R2, R4]

Examination asks whether the relevant records agree. Compare the matrix with the SSP, service descriptions, agreements, procedures, and evidence. If a responsibility appears in one record but not the others, determine whether the difference is legitimate or reflects an unresolved gap. Check versions and the actual service configuration, not only matching titles.

Interview asks whether the people can explain their work. Speak with the operator who performs the activity as well as the manager who approved the document. Ask what starts the task, what authority is needed, what happens when an input is missing, and where the result is recorded. An operator's uncertainty may reveal a training or procedure issue even when the written row is clear.

Testing asks whether the relevant mechanism or workflow behaves as described under the chosen conditions. Use approved test accounts, representative records, and controlled exercises. A denied access attempt can support a specific claim about a tested path. It does not automatically demonstrate every authorization, device, process, or application condition in the environment.

Record the Limits of the Conclusion

Document what was examined or tested, the conditions, observed result, and unresolved questions. A walkthrough conducted during business hours does not

establish that the overnight escalation route works. A test using one application does not prove that another application follows the same permission model.

The purpose of internal validation is to identify actionable weaknesses and support an honest readiness judgment. If the process fails, determine whether the cause is a missing assignment, inadequate authority, incorrect procedure, unavailable resource, technical defect, or weak evidence. The correction should address that cause rather than merely rewrite the row to match the failure.

6.34 Maintain the Matrix Through Changes and Provider Transitions

A responsibility matrix becomes inaccurate when the environment or service arrangement changes without a corresponding review. New applications, changed provider offerings, personnel turnover, office moves, acquisitions, altered information flows, and retired systems can all affect assignments. The change process should identify these triggers.

Harbor Point's system owner coordinates the review. The affected provider explains its changed contribution, application owners identify operational effects, and the evidence custodian evaluates record continuity. The approved change updates the matrix and its linked records where necessary. Minor administrative corrections and material service changes need not follow identical review paths, but both should be controlled appropriately.

Provider transitions deserve special attention because responsibilities may overlap for a period or become temporarily unassigned. Identify when the outgoing provider stops performing each task, when the incoming provider accepts it, and how the customer verifies continuity. A new contract start date does not prove that monitoring sources, administrative access, and evidence retrieval have transferred successfully.

The transition plan should address credentials, data, configuration records, open incidents, unresolved findings, retained evidence, and service dependencies relevant to the environment. Assign who authorizes transfers and verifies the receiving environment. A migration can change assessment scope or information handling, so the matrix review should connect to those decisions.

Close the Old Relationship Deliberately

After the new arrangement is verified, revoke or modify obsolete access, reconcile records, and preserve information that must remain available. Do not leave the outgoing provider with unnecessary administrative capability simply because the

migration is operationally complete. Conversely, do not terminate access needed for a required evidence transfer before an authorized preservation route exists.

The final transition record should identify what changed, when responsibilities transferred, what was verified, and which actions remain open. Future readers should be able to understand the current arrangement without reconstructing a series of informal messages between providers.

6.35 Recognize and Correct Common Matrix Failures

Every Row Says Shared

Shared can be accurate, but it is incomplete without the contribution of each party. Divide the activity into its decisions, actions, and handoffs. If the parties cannot describe those contributions, the row contains an unresolved allocation. Do not let a neutral-sounding label conceal the absence of an owner.

The MSP Owns Every Technical Requirement

An MSP may perform extensive technical work while the customer retains authorization, business context, personnel information, and oversight. Review each requirement for those dependencies. Assigning everything to the MSP can create tasks it cannot legitimately or practically perform, such as deciding an employee's project eligibility without customer input.

A Product Name Replaces the Implementation

A row naming a firewall, identity platform, or monitoring product identifies a technology, not a complete responsibility. Record who configures the capability, maintains the approved state, reviews results, resolves failures, and provides evidence. The product may support the work, but the service must still operate.

The Provider CRM Is Copied Without Adaptation

Provider documents describe a boundary and service assumptions. The customer must determine how its own implementation satisfies the assigned customer duties. Preserve the original provider document, then map those duties into the coordinated customer record. Do not rewrite the provider's responsibilities to fit a preferred answer.

Evidence Is Left Until Assessment Week

Late collection may reveal unavailable records, expired access, missing context, or a provider that cannot support the expected demonstration. Assign evidence production, custody, and access during process design. Confirm the route while there is time to correct a real limitation.

The Matrix Describes Aspirations as Current Practice

A proposed service, planned configuration, or unfilled role belongs in a clearly identified future or unresolved state. Keep it distinct from the approved operating arrangement. The customer should be able to tell which protections exist today and which actions remain necessary.

Signatures Replace Operational Verification

Approval demonstrates agreement within the signers' authority. It does not show that an account restriction works, an alert reaches the right person, or a recovery succeeds. Use appropriate examination, interviews, and controlled tests to evaluate the actual process. Preserve the difference between agreement and demonstrated operation.

6.36 Practice with Responsibility Scenarios

Scenario One The Manager Says Copy Another Employee

The service request identifies a new engineer and asks NorthStar to copy an existing employee's access. What should the matrix require? The request must be connected to an authorized project role and a valid approver. NorthStar should not interpret the request as approval for every accumulated permission on the model account. The customer clarifies the decision, the appropriate operator implements it, and the designated review checks the result.

Scenario Two The SOC Sends an Alert but Cannot Isolate the Device

Beacon's service includes analysis and escalation, but Harbor Point expected direct containment. The matrix should identify the agreed containment operator and authority. If that capability is absent, management must resolve the service or internal assignment. Changing Beacon's cell to responsible does not create technical access, contractual authority, or staff availability.

Scenario Three The Cloud Provider Assigns a Duty to the Customer

The provider CRM states that the customer must enable a relevant logging feature. Harbor Point assumed NorthStar's base subscription included all cloud administration. Compare the actual agreements, assign the task to a capable party, verify the configuration, and update the coordinated matrix. The provider's capability remains an input; the customer-side implementation must be completed.

Scenario Four The Training Portal Shows Incomplete Courses

NorthStar provides the platform and reports completion status, but several employees have not completed the assigned training. Harbor Point's designated manager or training coordinator must perform the agreed follow-up. The matrix should not imply that supplying a portal transfers the employer's management decisions to the MSP. Investigate whether the training population and assignments are also correct.

Scenario Five The Evidence Is in an Expiring Provider Portal

Harbor Point learns that its access to the outgoing provider's portal ends next week. The record contains material needed for the assessment evidence package. Identify the authorized custodian, applicable retention duty, permitted preservation route, and responsible provider contact. Preserve the relevant records with integrity and context before access ends; do not assume that an ordinary subscription archive satisfies the customer's obligation.

Scenario Six A Risk Owner Accepts a Missing Protection

A manager signs an internal exception because a legacy application cannot support the preferred configuration. The signature records a management decision. It does not establish that the relevant CMMC requirement is met or that a formal POA&M is permitted. The matrix should identify the actual condition, appropriate assessment treatment, corrective owner, and further decision required under the applicable rules.

Scenario Seven A Provider Changes Its Subcontracted Platform

NorthStar's monitoring supplier changes the platform supporting the service. Harbor Point should evaluate effects on data flows, service scope, access, retention, response, and evidence. The immediate provider remains responsible for explaining its agreed service, but the customer's matrix must reflect material changes to the contribution on which it relies. A corporate rebranding notice alone may not answer those questions.

Scenario Eight One Person Approves and Verifies Every Change

A small customer has limited staff. The answer is not to invent additional employees in the matrix. Identify actual roles, applicable separation-of-duties requirements, conflicts, and feasible review arrangements. Evaluate the design against the governing requirements. Where another qualified reviewer or changed process is necessary, make that need visible instead of using different role names for the same unchecked action.

Scenario Nine Nobody Owns the Restore Validation

NorthStar restores a project folder and reports success. Harbor Point later discovers that the recovered material is incomplete for the engineering task. The matrix needs a business validation owner as well as a technical operator. The approved restoration process should identify the intended information, destination, verification, and unresolved result. A successful job status supports only the work it actually confirms.

Scenario Ten The Matrix Is Green but the SSP Disagrees

The matrix names Beacon as the monitoring provider, while the SSP still describes an internal monitoring team that no longer exists. Reconcile the actual service arrangement, review its implementation and evidence, and correct the affected records. A green assignment status does not resolve contradictory documentation. Determine whether the inconsistency is limited to records or reflects missing operational work.

6.37 Conduct a Responsibility Workshop and Review the Chapter

A responsibility workshop should produce decisions and usable records. Invite participants who can explain the work and those who can authorize the allocation. Begin with the current scope and provider services. Use a few complete workflows to establish the method before mapping the remaining baseline systematically.

The facilitator should keep three questions connected: what must happen, who is authorized and able to make it happen, and what will demonstrate the result? When a participant identifies a limitation, record it as a decision or action rather than forcing agreement during the meeting. The workshop is useful when it exposes the missing work early.

A Practical Workshop Sequence

1. Confirm the assessed system, applicable baseline, source versions, and provider offerings.

2. Identify the customer roles, provider roles, decision authorities, and current contacts.

3. Map one complete access workflow and one complete monitoring or response workflow.

4. Decompose shared and inherited statements into specific contributions and conditions.

5. Assign verification, evidence production, custody, and provider evidence access.

6. Reconcile the proposed assignments with procedures, service agreements, and available resources.

7. Walk through normal events, failures, urgent changes, and an unavailable primary contact.

8. Record approvals, unresolved decisions, corrective actions, and ownership for maintaining the matrix.

These steps are a teaching method, not an official CMMC workshop requirement. The full assignment process must cover the actual applicable baseline and scope. Completing two example workflows is a way to learn and validate the method; it does not establish complete requirement coverage.

Applied Exercise

Create a responsibility package for a fictional engineering customer with eight employees, one internal application owner, an MSP, a monitoring provider, and a cloud repository. The customer also uses a physical office and an approved remote-work arrangement. Assume that the MSP administers identity and endpoints but does not administer the engineering application's internal roles.

Write a short description of the system and the provider boundaries. Then create twelve activity records covering project access, personnel changes, application identities, logging, alert escalation, incident decisions, configuration changes, vulnerability correction, restoration, training, physical entry, and assessment evidence. Each record should identify the authority, executor, trigger, verification,

evidence, and failure route. Map the relevant requirements and objectives using authoritative sources.

Introduce three problems: a provider cannot supply a promised evidence export, the primary customer approver is unavailable, and a new application feature changes the information flow. Explain how the package exposes each problem, who decides the response, and which records or technical arrangements must change. Keep proposed corrections separate from completed and verified implementation.

A strong submission allows another person to follow the workflow without inventing permissions or responsibilities. It also identifies the limitations of its examples and does not claim that twelve activity records constitute a complete CMMC assessment package.

Review Questions

1. What does the CMMC customer responsibility matrix explain about the relationship between a customer and an external service provider?

2. How does the coordinated customer matrix differ from the provider's own CRM?

3. Why should decision authority be distinguished from technical execution?

4. What information is missing when a row says only shared?

5. How can the assessment objectives reveal responsibilities hidden inside a broad requirement?

6. What makes a handoff complete, and why is sending a message not always sufficient?

7. How should the matrix distinguish assignment agreement from verified implementation?

8. What conditions must be explained before a customer relies on an inherited provider contribution?

9. How do operational log retention, incident preservation, and assessment-artifact retention differ?

10. Why does a monitoring service need a defined connection to incident decisions and response actions?

11. What should happen when the matrix assigns work excluded by the service agreement?

12. Why should a provider transition include evidence, credentials, open actions, and responsibility acceptance?

13. What can an internal walkthrough demonstrate, and what are its limits?

14. How does the matrix prepare the organization for the gap assessment in the next chapter?

Answer Guidance

For Questions 1 and 2, explain the service boundary and the customer's implementation. The provider CRM describes the relevant division between provider and customer. The coordinated matrix connects that division to the customer's internal roles and any other providers performing customer-side duties. Neither document should invent commitments for another party.

For Questions 3 through 5, focus on the work concealed by broad labels. A person who can configure access may not have authority to decide the business need. Shared must identify each contribution. Assessment objectives help separate the determinations that need support, such as identifying authorized populations and implementing the restrictions that apply to them.

For Questions 6 and 7, distinguish movement of a request from acceptance of responsibility and completion of the result. A handoff needs a recipient, usable input, and an acceptance condition. An agreed assignment can coexist with unfinished implementation or unavailable evidence. Internal tracking should preserve those distinctions.

For Questions 8 and 9, describe the exact provider service and the conditions of the contribution. Identify the customer tasks that remain. Explain each retention duty through its governing source, record population, trigger, and custodian. Do not convert the assessment-artifact period into a universal retention period for all operational data.

For Questions 10 through 12, connect the agreements to operating capability. Alerts need authorized recipients and response actions. Excluded work needs a real assignment and resources, not an optimistic cell entry. A provider transition needs verified acceptance of the relevant duties and continuity of records and access.

For Questions 13 and 14, describe internal validation honestly. It can reveal missing owners, failed handoffs, contradictory records, and technical defects under the conditions examined. It does not guarantee a certification outcome. Its findings

identify who can explain implementation, supply evidence, confirm a gap, and perform corrective work during the next phase.

Key Terms

Term	Meaning in this chapter
Customer responsibility matrix	Record describing customer and provider duties for the relevant services
Coordinated customer matrix	Customer record connecting internal roles with all relevant provider contributions
Decision authority	Role authorized to approve a particular decision
Executor	Person or service that performs the authorized activity
Verification	Check that the defined result occurred under stated conditions
Evidence custodian	Role responsible for controlled preservation and authorized retrieval of records
Handoff	Transfer of usable input and responsibility through an agreed route
Acceptance criterion	Condition used to determine that a handoff or result is sufficient
Inherited contribution	Provider-performed protection relied upon under identified conditions
Shared contribution	Activity whose completion depends on specifically described work by several parties
Assignment gap	Necessary work without an agreed capable and authorized owner
Service dependency	Capability or input supplied by another service that the workflow needs

Term	Meaning in this chapter
Internal readiness review	Organization's evaluation before assessment without claiming formal certification status
Affirming Official	Internal senior representative with the authority and duties identified in the CMMC rule

Closing Perspective

A useful responsibility matrix makes the security program understandable to the people who operate it. The customer can see which decisions it must make. The MSP can see which technical actions it has agreed to perform. Providers can explain their contributions and limits. Reviewers can follow the evidence without guessing how the pieces fit together.

The completed matrix should make it easier to answer a practical question: if this activity begins today, can the right people carry it through to an authorized, verified result? If the answer depends on an undocumented assumption, the responsibility work is not finished. If the answer is supported by clear roles, functioning handoffs, current records, and suitable evidence, the organization has a stronger basis for the next phase.

In Chapter 7, Performing the CMMC Gap Assessment, we will use that basis to compare the current implementation with the applicable requirements, evaluate the supporting evidence, and identify corrective work. Chapter 5 established the environment. Chapter 6 established who does the work. The gap assessment will examine how well that work satisfies the requirements and what remains to be addressed.

Official References

R1. 32 CFR 170.19, CMMC scoping. See the external service provider provisions, the customer responsibility matrix and SSP relationship, and the distinctions among assessment levels. Official annual CFR edition. Read official source

R2. 32 CFR 170.17, CMMC Level 2 certification assessment and affirmation requirements. See assessment procedures, external provider use, cloud offerings, and assessment-artifact retention and integrity. Official annual CFR edition. Read official source

R3. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The requirement baseline used for the Level 2 examples under the identified published framework. Read official source

R4. NIST SP 800-171A, June 2018, Assessing Security Requirements for Controlled Unclassified Information. See assessment objectives and the examination, interview, and testing methods. The potential evidence lists should not be treated as a mandatory checklist of every possible artifact. Read official source

R5. 32 CFR 170.22, Affirmation. See the internal Affirming Official role and the continuing-compliance affirmation provisions. Official annual CFR edition. Read official source

R6. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. See applicable reporting, preservation, cloud-service, and subcontract provisions. Read official source

R7. Electronic Code of Federal Regulations, 32 CFR Part 170. Check current amendments and the applicable contract and official program direction before relying on a specific assessment obligation. Read official source

Sources reviewed September 19, 2026. The examples explain responsibility design under the identified framework. They do not replace the official requirement text, contractual analysis, or the authorized assessment process.

CMMC for MSPs

From Readiness to Certification

Chapter 7

Performing the CMMC Gap Assessment

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and source context

7.1–7.7 Gap-assessment foundations and preparation

7.8–7.13 Evidence, interviews, testing, and finding logic

7.14–7.27 Level 2 requirement-family review

7.28–7.32 Provider, cloud, and MSP-specific assessment issues

7.33–7.36 Scoring, POA&M logic, prioritization, and remediation

7.37–7.39 Harbor Point gap-assessment case study

7.40–7.42 Validation workshop, scenarios, and chapter review

Key terms and official references

Chapter Purpose

A CMMC gap assessment is the point where preparation stops being a general conversation and becomes a disciplined comparison between what the organization is required to do and what it can actually demonstrate. The assessment is not a product scan, a policy inventory, or a questionnaire that asks whether the customer believes a safeguard exists. It is a structured effort to determine whether the applicable requirement and its assessment objectives are implemented within the defined scope, whether the implementation is operating as intended, and whether credible evidence supports that conclusion.

For an MSP, this work is especially important because the customer's implementation may depend on services, people, platforms, and records that cross organizational boundaries. A control can appear complete inside the customer's policy library while the technical work is performed by the MSP. The opposite can also occur: the MSP may operate a capable tool, but the customer has not made the policy decision, assigned the authorized population, retained the required evidence, or included the activity in the system security plan. A meaningful gap assessment must therefore connect the customer's obligations to the responsibility matrix developed in Chapter 6.

This chapter uses the fictional Harbor Point Engineering engagement. NorthStar Managed Technology provides managed IT services, Beacon SOC supplies monitoring support, and selected cloud services contribute infrastructure and application capabilities. The examples are intentionally practical. They show how an MSP can organize a readiness review, examine evidence, interview personnel, test mechanisms, record findings, separate confirmed gaps from assumptions, and convert the results into a remediation program that the customer can actually execute.

The objective is not to imitate or pre-judge an authorized CMMC assessment. Internal readiness work has a different purpose. It prepares the organization to understand its environment, correct weaknesses, improve evidence quality, and identify unresolved questions before those questions become assessment-day surprises. The organization should use authoritative sources, preserve the distinction between internal findings and formal assessment results, and avoid language that implies certification before an authorized assessment has occurred.

Learning Objectives

- Explain the difference between a CMMC gap assessment, a vulnerability assessment, an internal audit, and an authorized CMMC assessment.
- Establish a defensible assessment baseline by connecting the current scope, responsibility matrix, SSP, applicable requirement set, and assessment objectives.
- Use examine, interview, and test methods to evaluate implementation rather than relying on policy statements alone.
- Classify findings so that confirmed implementation gaps, evidence gaps, scope questions, documentation inconsistencies, and provider dependencies are not mixed together.
- Evaluate the 14 Level 2 requirement families from an MSP operational perspective without reducing them to a tool checklist.
- Identify provider and cloud-service contributions that must be substantiated through the exact service offering, customer responsibilities, and available evidence.
- Prioritize remediation according to security significance, dependency, feasibility, evidence impact, and contractual timing.
- Prepare internal findings for management review, remediation tracking, SSP updates, and later assessment preparation.

Source and Applicability Note

This chapter is written against the published CMMC framework in 32 CFR Part 170 and the Level 2 baseline that uses the 110 security requirements in NIST SP 800-171 Revision 2. The assessment approach refers to the June 2018 NIST SP 800-171A publication because that publication contains the assessment objectives and the examine, interview, and test methods associated with the Revision 2 requirement set. NIST has since issued newer revisions, but an internal readiness review must use the requirement and assessment sources incorporated by the applicable CMMC rule, solicitation, and contract rather than substituting a newer publication merely because it has a later date. [R1, R2, R3]

As of September 2026, the Department announced on July 13, 2026 that the transition to CMMC Phase II requirements was suspended while Phase I self-assessment requirements remain in place and the Department conducts a broader review. The

announcement did not remove the underlying obligation to safeguard covered defense information or eliminate applicable contractual cybersecurity duties. Organizations should therefore distinguish the current acquisition rollout status from the continuing need to implement and assess required safeguards. [R4]

The examples in this chapter are readiness-management examples. Terms such as red, yellow, green, severity, readiness score, evidence confidence, and remediation wave are internal management devices unless a cited governing source gives them a formal meaning. They should not be represented as official CMMC scores or certification determinations.

7.1 Start with a Baseline, Not with a Spreadsheet

A gap assessment becomes unreliable when the team opens a spreadsheet of requirements before confirming what is being assessed. The first question is not whether Requirement 3.1.1 is met. The first question is which system, locations, users, providers, and information flows are part of the environment to which the conclusion will apply. Chapter 5 established this scope and Chapter 6 assigned responsibilities. Chapter 7 must begin by freezing those working assumptions long enough to conduct a coherent review.

Harbor Point therefore creates an assessment baseline package before reviewing individual requirements. The package includes the current scope description, asset categories, network and data-flow diagrams, the SSP, the coordinated responsibility matrix, provider service descriptions, the applicable requirement source, the applicable assessment procedures, and a list of evidence repositories. The package is dated. If a material architecture change occurs during the review, the team records the change rather than silently assessing a moving target.

This baseline discipline prevents a common failure in MSP engagements: the evidence reviewer assumes that the environment is the same one described in last quarter’s diagram, while the service desk has already migrated endpoints, changed the identity provider, enabled a new remote-support tool, or moved backups to another service. An assessment that evaluates the wrong architecture can produce a technically careful but operationally meaningless result.

The baseline is not a declaration that every document is correct. It is the agreed starting point that the team will test. When the gap assessment discovers that the SSP, inventory, diagram, or responsibility matrix is inaccurate, the finding should identify

both the implementation fact and the documentation consequence. That separation helps the customer correct reality first and documentation second.

Working rule: Do not mark a requirement until you can state what environment, time period, and service arrangement the mark describes.

- Identify the exact Level and assessment type relevant to the customer’s current obligation.
- Record the assessed environment and the date on which the baseline was established.
- Collect the SSP, scope inventory, diagrams, provider descriptions, and responsibility matrix.
- Identify the authoritative requirement and assessment-procedure versions.
- Record known transitions or planned changes that may affect conclusions.

7.2 Understand What a Gap Assessment Can and Cannot Establish

An internal gap assessment can determine that evidence is missing, a configuration does not match the stated procedure, a required activity is not assigned, a control is implemented only for part of the scope, or personnel cannot explain the process they are expected to operate. These are valuable findings because they allow correction before an external review or contractual submission.

The same internal review cannot certify the organization, bind an assessor, or guarantee that a future authorized assessment will reach the same result. Differences in timing, evidence populations, sampling, system changes, interviews, and assessment judgment can affect conclusions. The internal team should therefore use language such as internal readiness conclusion, observed implementation, evidence reviewed, or remediation required rather than certified, passed CMMC, or assessor-approved.

This distinction is important for MSP sales and customer communications. A readiness service can be described as a structured assessment against the applicable requirement set and objectives. It should not be marketed as a shortcut to certification or as a promise that an authorized assessment organization will accept every internal conclusion. Precision protects both the customer and the MSP.

7.3 Build the Assessment Team Around Facts and Responsibility

A gap assessment needs people who understand both the requirements and the environment. A compliance specialist who cannot access the technical systems may misunderstand how a requirement is implemented. A senior engineer who knows every platform may overlook the need for authorization, documentation, retention, or management review. The most effective readiness teams combine governance, technical operations, business ownership, and evidence management.

At Harbor Point, the assessment lead coordinates the review but does not answer every question. NorthStar provides engineers who can demonstrate identity, endpoint, network, patching, and backup operations. Beacon supplies information about monitoring workflows and evidence available under the service agreement. Harbor Point contributes management, HR, application ownership, physical-security, and incident-decision roles. The SSP owner and evidence custodian participate throughout because changes discovered in one area often affect several documents.

The team should also separate implementation ownership from assessment judgment. A technician who built a configuration can explain it and provide evidence, but someone else should evaluate whether the evidence supports the assessment objective. This does not require a large organization to create artificial independence. It requires awareness of confirmation bias and a review process that challenges unsupported assumptions.

Role	Primary contribution	Common risk if missing
Assessment lead	Coordinates baseline, objectives, findings, and review sequence	Inconsistent methods and unresolved findings
Technical owner	Demonstrates configuration and operation	Paper-only conclusions
Business/process owner	Explains authorization and decision logic	Technical activity without approved purpose
Evidence custodian	Retrieves and preserves records	Last-minute evidence reconstruction
Provider representative	Explains external-service contribution and limits	Overstated inheritance or shared responsibility
Management reviewer	Accepts risk decisions and resources remediation	Findings with no authority to act

7.4 Create a Requirement-to-Objective Working Record

For Level 2 readiness work, a requirement sentence is only the beginning. NIST SP 800-171A decomposes requirements into assessment objectives that identify what the

assessor must determine. A broad requirement may therefore contain several distinct facts. Marking the entire requirement based on one artifact can conceal an unmet objective.

The working record should list the requirement identifier, each assessment objective, the responsible roles, the implementation description, expected evidence, actual evidence reviewed, interview targets, test steps, and the internal conclusion. It should also identify whether the conclusion applies to all in-scope assets or only a subset. This structure makes partial implementation visible.

For example, a customer may require multifactor authentication for privileged access and for network access to privileged and non-privileged accounts under the applicable Level 2 requirement. The team should not stop after seeing an MFA policy. It should identify the access paths, account categories, technology enforcement points, exceptions, emergency accounts, remote administration routes, and evidence showing that the requirement is applied to the relevant population.

7.5 Use Status Categories That Preserve the Nature of the Problem

A single red or green cell is attractive because it is easy to summarize, but it often destroys useful information. Harbor Point uses finding categories that describe why a conclusion is uncertain or incomplete. A confirmed implementation gap is different from an evidence gap. A scope question is different from a stale procedure. A provider dependency is different from an internal technical defect.

This distinction improves remediation. If the control is working but evidence is not retained, the corrective action may involve logging, report generation, retention, or evidence custody. If the process exists only in policy, the corrective action must change operations. If the evidence cannot be obtained from a provider, the solution may require a contract change, different service tier, alternate evidence source, or architectural decision.

Management can still create a dashboard, but the underlying register should preserve these categories. The dashboard should never make an unknown look equivalent to a verified implementation.

Internal category	Meaning	Typical next action
Implemented / supported	Observed implementation and sufficient internal support for the objectives reviewed	Maintain and monitor
Implementation gap	Required activity or mechanism is	Design and implement correction

	absent or materially incomplete	
Evidence gap	Implementation may exist but current evidence is insufficient	Improve collection, retention, or retrieval
Documentation gap	Implementation and controlled documentation disagree or are incomplete	Reconcile SSP, procedure, diagram, or inventory
Scope question	Applicability or boundary is unresolved	Return to scoping analysis
Provider dependency	Conclusion depends on external-service information or capability not yet substantiated	Obtain provider evidence or redesign dependency
Not yet evaluated	Objective has not received sufficient review	Schedule assessment work

7.6 Plan Evidence Before Requesting It

Evidence requests should begin with a hypothesis about what would demonstrate the objective. Asking a technician to send everything related to access control usually produces a large folder with screenshots, exports, tickets, and policies that are difficult to connect to specific determinations. A better request identifies the objective, the relevant population, the time period, and the expected evidence types.

For recurring processes, the team should consider whether one sample demonstrates only that an event happened once or whether the review needs a population and selected examples to understand sustained operation. A single closed termination ticket does not establish that all terminated users were disabled promptly. A current configuration screenshot does not show how exceptions were approved over the prior months. The evidence plan should match the claim being made.

Evidence should also be attributable. The reviewer should know which tenant, system, asset, account, report, or customer the artifact describes. MSP environments often aggregate data from many customers. A dashboard export that cannot be tied reliably to Harbor Point can create more questions than confidence.

7.7 Set the Assessment Calendar Around Dependencies

The review sequence should follow dependencies rather than the order in which controls appear in a spreadsheet. Identity and asset inventory influence access, logging, configuration, incident response, and vulnerability management. Provider evidence may need lead time. Interviews may reveal implementation details that should be tested before the team closes a finding.

Harbor Point therefore begins with scope, inventory, identity, architecture, and shared-service dependencies. It then reviews technical control families, cross-cutting operational processes, and finally documentation reconciliation. This sequence reduces rework. If the team discovers midway that a remote-management platform belongs in scope, it can still update the assessment plan before dozens of conclusions have been finalized.

A practical calendar includes evidence-request dates, owner interviews, technical demonstrations, finding-review meetings, remediation decision points, and a final management readout. The schedule should leave room for re-testing corrections instead of treating remediation as work that happens after the assessment report is finished.

7.8 Apply Examine, Interview, and Test as Complementary Methods

The assessment methods in NIST SP 800-171A are examine, interview, and test. Each method answers a different kind of question. Examine evaluates documents, records, settings, outputs, and other artifacts. Interview determines whether responsible people understand and perform the activity. Test exercises or observes a mechanism or process to determine how it behaves. Strong readiness work uses the methods together rather than treating one as universally superior. [R2]

A procedure may be perfectly written while the service desk follows a different workflow. An engineer may describe a technically sound control that is disabled on a subset of endpoints. A test may show that an account is blocked correctly but not establish who authorized the restriction or whether exceptions are reviewed. Triangulation turns these separate observations into a defensible internal conclusion.

The objective determines which methods add value. For a physical visitor process, examine and interview may be central, while a technical test may be limited. For session lock, authentication enforcement, logging, or network boundary protections, technical observation can be especially useful. The team should avoid performative testing that adds risk without increasing confidence.

7.9 Assess the Implementation, Not the Product Name

CMMC requirements describe outcomes and conditions, not approved commercial product lists. An MSP may use a respected EDR, SIEM, RMM, identity, or backup platform and still implement the relevant requirement incorrectly. Conversely, a

smaller organization may satisfy a requirement with a carefully configured service and disciplined process even if the product is not marketed as a compliance platform.

During the gap assessment, the reviewer should translate every product claim into an implementation claim. Instead of EDR covers malware protection, ask which in-scope systems have the agent, which protection capabilities are enabled, how health is monitored, how exclusions are governed, how alerts are handled, and what happens when the agent stops reporting. This turns brand confidence into observable evidence.

For MSPs, product boundaries are particularly important because one console can manage multiple customers. The assessment must show Harbor Point's configuration and records without exposing another customer's data or assuming that global MSP defaults are identical to the customer-specific policy.

7.10 Evaluate Evidence Quality, Not Just Evidence Existence

Evidence has dimensions of quality. It should be relevant to the objective, attributable to the assessed environment, sufficiently current for the claim, authentic enough for the internal review, complete enough to support the determination, and retrievable by an authorized person. An artifact can exist and still fail several of these tests.

Consider an MFA screenshot captured from an identity portal. It may show that an authentication method exists, but not which users are covered, which conditional-access policy enforces it, whether privileged break-glass accounts are excluded, or whether another remote path bypasses the portal. The reviewer should identify exactly what the screenshot proves and what remains to be demonstrated.

The team should also distinguish source evidence from presentation evidence. A slide deck that summarizes a configuration may be useful for management, but the underlying policy export, configuration record, log, or system observation usually provides stronger technical support. Internal assessment files should preserve enough context that a later reviewer can understand how the conclusion was reached.

7.11 Conduct Interviews That Follow Real Work

Interviews are most useful when they follow an event. Ask the service desk to explain what happens when a new engineer needs project access, when a privileged technician leaves NorthStar, when a vulnerability cannot be remediated immediately, when a SOC alert arrives at 2:00 a.m., or when a backup restoration is requested.

Event-based questions reveal handoffs, decision authority, exceptions, and evidence creation.

Avoid turning the interview into a vocabulary exam. The goal is not to test whether technicians can quote requirement numbers. The goal is to determine whether the organization has a repeatable process that satisfies the requirement and whether the people performing it understand their role. A technician who can explain the process clearly in operational language may provide stronger evidence than one who memorized a policy sentence.

Record contradictions as findings to investigate, not as reasons to blame the interviewee. If three technicians describe three different approval paths, the gap may be process ambiguity rather than individual failure. Follow the discrepancy into tickets, procedures, and configuration until the team understands what actually happens.

7.12 Design Tests That Are Safe, Reproducible, and Relevant

Testing should have a defined question and a safe method. A readiness team can observe that an unauthorized account is denied access, verify that a session locks after the configured interval, inspect that audit events are generated, confirm that a disabled account cannot authenticate, or test restoration using an approved non-production dataset. It should not create unnecessary operational risk merely to produce dramatic evidence.

Before testing, identify the expected result, the system or account used, approvals needed, rollback method, and evidence to capture. After testing, record the actual result and any limitations. A successful test on one workstation does not automatically establish coverage for every workstation, server, cloud resource, and remote path. The population and configuration model determine how far the result can reasonably support the internal conclusion.

MSPs should be especially careful with shared platforms. Testing must not affect other tenants or expose another customer’s data. Where a provider does not permit direct testing, the customer may need provider assurance, documented service behavior, customer-side observation, or an alternate architecture.

7.13 Write Findings That Someone Can Correct

A useful finding describes the condition, the requirement or objective affected, the evidence examined, the observed gap, the scope of the issue, and the likely corrective owner. It avoids vague statements such as improve MFA or update policies. Those phrases do not tell a technician what is wrong or tell management what decision is needed.

For example: Harbor Point’s remote-support workflow requires MFA through the primary identity provider, but two local emergency administrator accounts used by NorthStar are not governed by that mechanism and no compensating approved access process was demonstrated. That statement identifies the path, accounts, responsibility, and evidence problem. The remediation can now address emergency access design, monitoring, authorization, and documentation.

The finding should also record uncertainty. If the team has not yet obtained provider evidence, say that the conclusion is pending rather than marking the requirement failed based on absence of documentation in the customer repository. Internal rigor depends on distinguishing not observed from observed not implemented.

7.14 Access Control

Access control is where the responsibility matrix becomes operational. The team should identify authorized users, permitted functions, remote paths, privileged roles, wireless access, external connections, portable devices, and information-flow restrictions. Reviewers should trace approval to account or role implementation and then to verification. For MSP administration, include RMM access, remote shells, local administrator credentials, service accounts, emergency access, and any customer-side approval that technicians rely upon.

Common gaps include excessive inherited permissions, stale accounts, shared administrative identities, remote access that bypasses the primary MFA path, and tickets that request access without documenting business authorization. Evidence can include access requests, role assignments, identity-provider configuration, privileged-access records, remote-session logs, group membership exports, network rules, and completed access reviews.

For access control, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and

what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

A useful family-level review ends with three outputs: confirmed strengths that should be maintained, objective-level gaps requiring corrective action, and unresolved questions that must be answered before the family can be considered internally supported. This approach prevents the organization from turning a broad family discussion into an unsupported yes-or-no judgment.

7.15 Awareness and Training

Training readiness is not demonstrated by owning a training platform. Determine which personnel require security awareness, role-based instruction, and information-handling guidance; when training occurs; how completion is tracked; and what happens when someone does not complete it. MSP personnel who can access the customer environment need training consistent with their responsibilities and contractual arrangements.

Gap assessments should compare training populations with actual privileged and support personnel. Contractors, temporary workers, and newly assigned technicians are common places where the roster and the technical access population diverge. Evidence should connect the person, required curriculum, completion date, and follow-up process.

For awareness and training, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.16 Audit and Accountability

Audit readiness requires the organization to know what events matter, which systems generate them, where they are collected, how clocks and identities support interpretation, who reviews them, and what happens when logging fails. A SIEM subscription is only one component. The gap assessment should examine log-source coverage, alert rules, retention, review workflows, privileged activity, and protection of audit information.

For an MSP, check whether the customer can obtain evidence from shared monitoring services and whether customer-specific logs are attributable. Missing endpoint telemetry, disabled audit categories, expired collectors, inconsistent time settings, and provider retention limits often create evidence and implementation gaps at the same time.

For audit and accountability, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.17 Configuration Management

Configuration management connects approved baselines to real systems. Review the source of secure configurations, change authorization, exception handling, software restrictions, inventory updates, and mechanisms used to detect drift. The team should sample normal changes and emergency changes and determine whether approval, implementation, validation, and documentation are all present.

MSP automation can strengthen this family when scripts, policies, and profiles are controlled. It can also amplify mistakes when global changes are pushed without customer-specific review. Evidence should identify versions, approvals, targets, success or failure results, and remediation of exceptions.

For configuration management, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.18 Identification and Authentication

The gap assessment should map every meaningful identity path: workforce identities, privileged accounts, service accounts, devices, local accounts, application identities, remote-support identities, and emergency credentials. Determine how identities are uniquely assigned, authenticated, protected, revoked, and reviewed. Password policy alone does not answer these questions.

MFA enforcement needs special attention because diagrams often show one primary access path while administrators know several alternatives. Test customer portals, VPN, cloud consoles, RMM, local elevation, hypervisor management, and recovery accounts as applicable. Record exclusions and verify that they have a defined security purpose and compensating management.

For identification and authentication, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.19 Incident Response

Incident response is a chain of detection, triage, decision, containment, reporting, preservation, recovery, and lessons learned. The gap assessment should compare the written plan with recent incidents or exercises. Determine who may declare an incident, who can isolate systems, who contacts legal or contract personnel, how provider notifications are handled, and how evidence is preserved.

MSP and SOC contracts often contain notification language that is too general for an operational response. Review actual escalation routes, after-hours contacts, containment authority, and customer decision points. Tabletop exercises should expose uncertain handoffs before a real event does.

For incident response, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.20 Maintenance

Maintenance controls apply to authorized maintenance activities, tools, personnel, and remote methods. The team should identify vendor support channels, remote maintenance sessions, temporary accounts, diagnostic tools, and procedures for removing or sanitizing equipment when required. Maintenance is often overlooked because ordinary IT support feels routine.

MSP remote administration belongs in this discussion when it performs maintenance functions. Assess who can initiate sessions, how the session is authenticated, whether actions are attributable, how customer authorization is represented, and how temporary access is terminated.

For maintenance, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.21 Media Protection

Media protection extends beyond USB drives. Identify digital and physical media containing CUI, backup media, exported reports, removable devices, printed material, and disposal processes. Determine who may transport or access media, how it is protected, and how sanitization or destruction is verified.

Cloud-centric customers may believe they have no media problem while employees print drawings, export CSV files, download email attachments, or receive replacement storage devices. The gap assessment should follow information into those edge cases instead of limiting the review to formal removable-media inventories.

For media protection, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.22 Personnel Security

Personnel security connects HR decisions to technical and physical access. Review screening, role changes, transfers, terminations, sanctions, and notification paths. The important operational question is whether personnel events reliably trigger the right security actions and whether those actions are completed and verified.

MSP personnel changes matter when technicians hold customer-specific or shared administrative privileges. The customer should understand how the provider controls onboarding, termination, role changes, and continued need for access. Provider statements should be supported at the level the customer relies upon.

For personnel security, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.23 Physical Protection

Physical protection should be assessed at every location where relevant systems, devices, media, or printed CUI are used or stored. Examine authorization, visitor control, physical access records, alternate work sites, device protection, and responsibilities for remote work. A secure data center does not protect a laptop left in an uncontrolled home environment.

MSPs should distinguish customer facilities from provider facilities and cloud facilities. Each boundary may use different evidence and responsibility. The customer SSP and responsibility matrix should accurately describe what is inherited, what remains local, and what is handled through policy at alternate work sites.

For physical protection, Harbor Point’s internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.24 Risk Assessment

Risk assessment readiness includes periodic organizational risk evaluation and vulnerability scanning as required by the applicable baseline. The team should determine the defined frequencies, scope, authentication level, asset coverage, applications included, response process, and verification of remediation.

A vulnerability scanner can report thousands of findings without proving that the process works. Review asset coverage, excluded systems, credential failures, false-positive handling, aging, approved exceptions, and rescans. MSP service tiers should be compared with the customer's required scope and remediation expectations.

For risk assessment, Harbor Point's internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.25 Security Assessment

Security assessment requires the organization to evaluate controls, develop and manage corrective actions, monitor security controls, and maintain the SSP. This chapter's gap assessment directly supports that discipline, but the readiness exercise should not be confused with the customer's formal recordkeeping obligations.

Examine prior assessments, open plans of action, management reviews, control-monitoring records, and SSP updates. Determine whether closed items were actually re-tested. A ticket marked complete is not the same as a verified corrective action.

For security assessment, Harbor Point's internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.26 System and Communications Protection

This family addresses architectural and communications protections such as boundary protection, information transfer, network separation, cryptographic mechanisms, session protections, collaborative devices, and key management. The gap assessment should use diagrams and live configuration together. A firewall drawing that does not match routing, cloud security groups, or remote-access paths is a documentation and implementation risk.

MSPs should review administrative tunnels, site-to-site connections, DNS and email security dependencies, cloud integration, remote-support channels, encryption use, and key or certificate ownership. Provider features are relevant only when enabled and configured for the assessed environment.

For system and communications protection, Harbor Point's internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.27 System and Information Integrity

System integrity combines flaw remediation, malicious-code protection, security advisories, monitoring, and response to suspicious or unauthorized conditions. The team should follow the lifecycle from vulnerability or alert discovery to correction and verification. Tool deployment percentages should be reconciled with the actual in-scope asset inventory.

Common gaps include unhealthy endpoint agents, overdue patches, exclusions without approval, unmanaged appliances, delayed remediation with no risk decision, and advisories that are received but not evaluated. Evidence should show coverage, exceptions, corrective action, and confirmation that the issue is resolved.

For system and information integrity, Harbor Point's internal reviewer records both the control implementation and the evidence path. The reviewer asks who owns the requirement, which NorthStar or Harbor Point workflow performs it, how the result is verified, and what records can be produced without reconstructing history. When an external service contributes, the exact offering and customer-side prerequisites are documented rather than labeling the entire family inherited.

7.28 Assess MSP Administrative Platforms as Part of the Customer Story

RMM, PSA, documentation, remote-support, privileged-access, backup, and security platforms can become central to a customer's implementation even when they are owned by the MSP. The gap assessment should identify what each platform can do to the customer environment, what data it stores, which identities can use it, how access is monitored, and how customer-specific evidence can be retrieved.

A platform with broad administrative reach deserves special attention. If compromise of the MSP console could change customer security settings, deploy software, access credentials, or open remote sessions, the customer's security story cannot treat the console as irrelevant merely because it sits outside the customer tenant. Scope and external-service rules should be applied according to the official framework and actual architecture. [R1]

The readiness team should also test operational separation. Can a technician assigned to another customer see Harbor Point? Are customer credentials stored in a shared vault with appropriate authorization boundaries? Are global administrators limited and reviewed? Are emergency MSP privileges recorded? These questions connect provider governance to customer risk.

7.29 Evaluate External Service Provider Evidence Without Overclaiming Inheritance

When a cloud service, security provider, or MSP performs part of the implementation, the internal assessor should identify the exact contribution and the conditions under which the customer relies on it. Provider marketing, a general compliance page, or a certificate for a different service offering may not establish the customer's implementation.

Review the provider's customer responsibility matrix or equivalent documentation, service description, relevant assurance artifacts, contractual commitments, configuration requirements, region or tenant conditions, and customer-side responsibilities. Map those facts back to the customer SSP and coordinated responsibility matrix.

If required evidence is unavailable, do not invent it. Record the provider dependency, determine whether another authoritative artifact can support the objective, consider whether the service agreement can be changed, and evaluate whether the architecture should be adjusted. An unknown provider contribution is a management issue that should remain visible.

7.30 Assess Cloud Services at the Selected Offering and Tenant Configuration

Cloud assessment should occur at the offering and tenant level, not the vendor-name level. Identify the service model, region, selected features, identity configuration,

logging, encryption, backup, administrative roles, customer-managed settings, and external integrations. The provider may protect the underlying service while Harbor Point remains responsible for tenant configuration and user behavior.

For services used to process, store, or transmit CUI, apply the current official CMMC and contractual requirements to the selected cloud arrangement. The gap assessment should record what assurance the customer relies upon and which obligations remain with Harbor Point and NorthStar. Do not extrapolate a provider-wide statement to a service that has different authorization, support, or data-handling characteristics.

Cloud configuration evidence can change quickly. Preserve dated exports or reports, configuration snapshots, identity records, and provider documentation versions when they materially support the internal conclusion. A screenshot without tenant identity, date, or configuration context should be treated cautiously.

7.31 Test the Evidence Retrieval Process Before Assessment Day

A mature environment can still struggle during assessment preparation if evidence is difficult to retrieve. The gap assessment should therefore include an evidence-retrieval exercise. Select representative objectives and ask the assigned custodian to produce the expected records using the normal process and access rights.

Measure whether the evidence can be found, whether it is attributable to Harbor Point, whether the time period is clear, whether sensitive information is handled appropriately, and whether another person can understand the artifact without oral translation from the engineer who created it. Retrieval problems often reveal undocumented dependencies on one employee or one provider portal.

NorthStar creates a controlled evidence index that points to authoritative repositories rather than duplicating every record into a single folder. Where copies are retained for assessment purposes, the team applies access control, naming, versioning, and retention rules so that the evidence repository itself does not become an unmanaged store of sensitive information.

7.32 Reconcile the Gap Assessment with the SSP and Responsibility Matrix

Every material finding should prompt a documentation check. If the actual environment differs from the SSP, decide whether the implementation or the SSP must change. If a responsibility is performed by a different party than the matrix

states, correct the assignment only after confirming the real operating arrangement. The goal is not to make the paperwork agree with itself; the goal is to make the paperwork accurately describe a compliant implementation.

Harbor Point maintains a reconciliation log linking each gap to affected documents. A network boundary change may require updates to diagrams, the SSP, asset inventory, provider descriptions, and procedures. A new SOC escalation model may affect the responsibility matrix, incident plan, contact list, and evidence process. Recording these connections reduces the chance that remediation fixes technology while leaving contradictory documentation behind.

7.33 Use CMMC Scoring Rules Carefully in Internal Readiness Work

Organizations often want a single number because it appears to make progress measurable. Internal teams should be careful not to invent a score and label it a CMMC score unless they are applying an applicable official scoring methodology correctly and in the proper context. A readiness dashboard can show counts of objectives reviewed, confirmed gaps, evidence gaps, or remediation status without pretending to be an authorized assessment result.

When the applicable process requires a specific score or SPRS submission, use the governing methodology and current official instructions. Keep internal confidence measures separate. A high percentage of objectives reviewed does not necessarily mean high security readiness if the remaining gaps affect critical access, incident, authentication, or boundary protections.

Management metrics should therefore answer operational questions: Which requirements remain unsupported? Which gaps affect many assets? Which findings depend on provider action? Which corrections require architecture change? Which items can be re-tested now? These measures drive work rather than creating false precision.

7.34 Understand POA&M Eligibility and the Difference Between Planned and Implemented

A plan of action and milestones is a management tool for defined corrective work; it does not transform an unmet requirement into an implemented one. CMMC rules place conditions on when POA&Ms may be used and which requirements or scoring conditions affect eligibility. The readiness team should confirm the current official provisions rather than assuming that every gap can be deferred. [R1]

Internally, Harbor Point records corrective actions for every gap whether or not the item would qualify for treatment under a formal CMMC POA&M process. This broader remediation register helps management track architecture, policy, evidence, provider, and documentation work. Formal POA&M status is applied only when the governing process allows it.

Each corrective action includes an owner, required resources, dependencies, target date, validation method, and closure evidence. Closure occurs after re-testing or re-examination demonstrates the intended result. The phrase fixed in production is not accepted as sufficient closure evidence by itself.

7.35 Prioritize Remediation by Security Effect and Dependency

A remediation plan should not simply sort by requirement number or by which tasks are easiest. Harbor Point evaluates security significance, exposure, number of affected assets, dependency on other controls, contractual timing, evidence consequences, operational disruption, and implementation effort. The purpose is to reduce meaningful risk while building a sequence that can actually be executed.

Identity, asset inventory, architecture, and privileged access often have high dependency value because many other controls rely upon them. Fixing an isolated template issue may be useful, but it should not delay correction of an unmanaged administrative path. Similarly, replacing a platform may take months, so the team should identify interim risk treatment and evidence while the larger project proceeds.

NorthStar groups remediation into waves. Wave One addresses conditions that create immediate access, exposure, or widespread control failure. Wave Two addresses foundational process and architecture work. Wave Three improves evidence reliability, documentation consistency, automation, and long-term sustainment. This is an internal planning model, not an official CMMC priority scheme.

Priority factor	**Question**
Security significance	What could happen if the gap remains?
Coverage	How many in-scope assets, users, or workflows are affected?
Dependency	Which other requirements rely on this correction?
Time sensitivity	Is there a contractual, operational, or assessment deadline?
Provider dependency	Does another organization need to act or supply evidence?
Validation effort	How will the team prove the correction works?

7.36 Build a Remediation Record That Supports Re-Testing

Every remediation item should begin with the original finding and end with objective evidence of closure. The record should preserve the affected requirement or objective, root cause when known, corrective design, implementation steps, change approvals, test plan, actual test result, residual issues, documentation updates, and closure approval.

Root cause matters because repeated technical fixes can conceal a process failure. If new users repeatedly receive excessive permissions, the problem may be the access request form, role design, technician training, copied permissions, or lack of verification. Correcting one account does not correct the system that produced the account.

Re-testing should be performed against the same outcome the finding described. If the issue was incomplete endpoint coverage, the team should reconcile the current in-scope asset inventory with active protection and investigate exceptions. If the issue was inaccessible provider evidence, the team should demonstrate the new retrieval process rather than merely recording that the contract was amended.

7.37 Harbor Point Case Study: Establish the Internal Assessment Baseline

Harbor Point begins its gap assessment with a controlled baseline dated September 2026. The team confirms the in-scope engineering enclave, approved remote-work devices, cloud repository, identity service, managed endpoints, boundary devices, backup service, NorthStar administration platforms relevant to the customer, and Beacon monitoring relationship. The current SSP and responsibility matrix are included even though the team expects to find inconsistencies.

The assessment lead maps the 110 Level 2 requirements and their objectives into a working register. Each objective has a responsible participant, planned evidence, interview target, and test method where appropriate. Provider-dependent objectives are tagged so that requests can be sent early. The team records the July 2026 Phase II suspension as acquisition context but continues the readiness review because Harbor Point’s underlying contractual safeguarding responsibilities and Phase I obligations still require disciplined implementation.

The first week focuses on identity, inventory, architecture, access, logging, and provider evidence. This produces several cross-cutting findings before the family-by-

family review begins. The team discovers three former NorthStar technicians whose customer-specific roles were removed but who still belong to a shared support group capable of initiating a limited session. It also finds that two engineering laptops are missing from the EDR console because they were rebuilt using an old deployment process.

7.38 Harbor Point Case Study: Record Findings Without Hiding Uncertainty

The team classifies the shared support-group issue as a confirmed implementation gap because membership and access behavior can be demonstrated. The missing EDR devices are also a confirmed implementation gap. A third issue involves the cloud provider’s retention evidence. Harbor Point’s policy states that required audit information is retained according to the approved logging plan, but the team cannot yet obtain a report showing the configured retention period for one service. That item is recorded as a provider evidence dependency pending further review rather than automatically declared failed.

An incident-response interview reveals another problem. Beacon’s escalation procedure says that critical events are sent to NorthStar’s on-call engineer, while Harbor Point’s incident plan says the SOC contacts Harbor Point’s security coordinator directly. Recent tickets show both patterns. The team records a workflow/documentation inconsistency with potential incident-response impact and schedules a joint walkthrough to determine the actual authorized model.

These categories matter during management review. The access and endpoint findings require immediate technical correction. The logging item requires provider information and may or may not reveal an implementation defect. The incident item requires an authority decision, agreement update, procedure reconciliation, and exercise. One dashboard color would not have conveyed these different corrective paths.

7.39 Harbor Point Case Study: Remediate, Re-Test, and Update the Security Story

NorthStar removes the unnecessary shared support memberships, reviews the complete privileged support population, and implements a customer-specific approval check for future membership. Harbor Point and NorthStar then test that a removed technician cannot initiate a session and preserve the relevant group export, approval

record, and test result. The endpoint team rebuilds deployment automation, reconciles the asset inventory with the protection console, restores EDR coverage, and documents the exception-detection process.

The cloud provider supplies tenant-specific retention information and Harbor Point confirms that the configured service meets the internal logging design for the relevant data. The evidence dependency is closed with the provider record, tenant configuration, and SSP reference. For incident response, Harbor Point chooses a single escalation model: Beacon notifies NorthStar for technical triage while Harbor Point retains defined incident decision authority. Contracts and procedures are reconciled, and the parties conduct a tabletop exercise that includes an after-hours alert and unavailable primary contact.

The gap assessment closes only after these corrections are re-tested and documentation is updated. The result is not a certification statement. It is a stronger, internally supported implementation package with fewer unknowns, clearer responsibilities, and evidence that can be retrieved. That is the practical value of readiness work.

7.40 Run a Gap-Assessment Validation Workshop

Before finalizing the internal report, conduct a validation workshop with the people who own the most significant findings. The workshop should verify that findings describe the current environment, owners agree on the facts, proposed actions are feasible, provider dependencies are understood, and closure criteria are specific enough to support re-testing.

Do not use the workshop to negotiate inconvenient findings away. If management disagrees with a conclusion, return to the objective and evidence. The finding may be corrected, narrowed, or reclassified when new facts justify the change. It should not disappear merely because the remediation is expensive.

The final internal readout should separate current implementation status from the remediation roadmap. Management needs to know what is true now, what work is approved, what remains dependent on another party, and which changes could alter scope or architecture.

- Confirm the assessment baseline and material changes during the review.
- Review every high-impact confirmed gap and every unresolved scope question.

- Verify that provider-dependent conclusions identify the exact missing fact or artifact.
- Confirm remediation owners, dependencies, validation methods, and document updates.
- Schedule re-testing and management follow-up before declaring readiness work complete.

7.41 Applied Scenarios for MSP Readiness Teams

Scenario One - The Green Dashboard. NorthStar's security dashboard reports 99 percent endpoint coverage. The missing one percent is a domain controller used in the engineering enclave. The readiness team should not accept the aggregate percentage as sufficient. Reconcile expected assets to reporting assets, determine why the domain controller is missing, assess the security effect, restore coverage if appropriate, and record the exception and validation.

Scenario Two - The Perfect Policy. Harbor Point's account-management procedure requires manager approval and quarterly access review. Interviews reveal that service desk staff accept email requests from any department supervisor and no one can produce the last quarterly review. This is not primarily a writing problem. The assessment should identify the operational and evidence gaps, assign corrective ownership, and then update the procedure if the approved workflow changes.

Scenario Three - The Provider Certificate. A cloud provider has a respected compliance certification, but Harbor Point cannot determine whether the selected service tier and region are covered or what customer responsibilities remain. Record the provider dependency, obtain service-specific assurance and responsibility documentation, and do not mark the customer implementation complete based only on the provider's brand.

Scenario Four - The Emergency Account. An emergency local administrator account is excluded from the normal MFA path. The team should examine why it exists, how credentials are protected, who may use it, how use is detected and reviewed, whether the design is allowed by the applicable requirement, and what alternative architecture or controls are available. The word emergency does not remove the account from the assessment.

Scenario Five - The Closed Ticket. A vulnerability ticket is closed because a patch was deployed. The subsequent scan still shows the vulnerability on two servers.

Closure should depend on the defined validation result, not on the completion of the deployment task. Reopen the corrective action, investigate the failed systems, and preserve the rescan evidence.

7.42 Chapter Review and Readiness Checklist

A CMMC gap assessment should leave the organization with greater clarity, not merely a larger spreadsheet. The team should understand what environment was reviewed, what evidence supports each conclusion, where responsibilities cross organizational boundaries, which gaps are confirmed, which questions remain open, and how corrections will be validated. The readiness package should also make it easier to maintain the environment after the immediate assessment effort ends.

For MSPs, the most important lesson is that readiness is a service-delivery discipline. Access approvals, remote administration, logging, patching, vulnerability management, incident escalation, backup, personnel changes, and evidence retrieval occur throughout the year. If those workflows are clear and repeatable, assessment preparation becomes an organized demonstration of normal operations. If they are improvised, the assessment exposes the improvisation.

The next chapter can build on this foundation by turning confirmed gaps into an implementation and remediation roadmap with sequencing, project governance, resource decisions, and sustainable evidence production. The goal is not to prepare for one assessment day. The goal is to operate an environment that can continue to protect information and demonstrate that protection over time.

- Baseline and scope are dated and understood.
- Every reviewed objective has traceable evidence or an explicit unresolved status.
- Implementation gaps are separated from evidence and documentation gaps.
- Provider dependencies are tied to exact services and customer responsibilities.
- High-impact findings have approved corrective owners and validation methods.
- Closed findings have been re-tested.
- SSP, diagrams, inventories, procedures, and responsibility records are reconciled.
- Management understands current status separately from planned future work.

Detailed Level 2 Assessment Field Guide

The following field guide expands the family-level discussion into a practical readiness method. It is designed for an MSP-led internal assessment team that needs to know what to examine, whom to interview, what to test, and which failure patterns deserve attention. It is not a substitute for the applicable NIST SP 800-171A assessment procedure. Instead, it helps the team organize operational evidence around those objectives and translate broad requirements into observable work.

Each family should be assessed against the actual scope and responsibility allocation. The examples below assume a mixed environment in which Harbor Point retains business authority, NorthStar performs selected technical administration, Beacon provides monitoring, and cloud providers contribute defined service capabilities. A different customer may allocate the work differently. The evidence must follow the real implementation, not the example.

Field Guide 1: Access Control

Access Control should be evaluated as an end-to-end authorization system. Begin with the population of people, devices, services, and external connections that can reach the assessed environment. Then determine how business authorization becomes a technical account, role, network path, application entitlement, remote session, or information-flow rule. The assessment should be able to explain who requested access, who was authorized to approve it, who implemented it, what restrictions applied, and how the organization verified that access remained appropriate.

MSP environments frequently create access paths that are absent from customer diagrams. RMM consoles, remote shells, shared vaults, local break-glass accounts, hypervisor portals, backup consoles, and vendor support accounts should be included when they can administer or expose the assessed system.

Suggested assessment methods

Method	Readiness focus
Examine	Current user and privileged-account lists; group and role exports; access request records; remote-access configuration; firewall or access-control rules; application permissions; privileged-access records; account review results; termination records; exception approvals. RMM and remote-support role configuration; local administrator populations; emergency-access procedures; service-account inventories; third-party connection

	records; customer-specific access groups.
Interview	Business managers who approve project access; service desk personnel who provision accounts; NorthStar administrators; application owners; personnel responsible for periodic access reviews. Ask how urgent requests are handled, how temporary access expires, how technicians avoid copying excessive permissions, and what happens when the normal approver is unavailable.
Test	Select representative users and compare approved need to actual permissions. Attempt an approved negative test using an account that should not have access. Observe remote-support authentication and session attribution. Verify that a terminated or removed account cannot use relevant access paths.

Common MSP/customer failure patterns

- Shared technician accounts or generic local administrator credentials.
- Former technicians remaining in shared support groups.
- Customer approval recorded only in informal email or chat with no attributable decision.
- MFA applied to the main portal while another administrative path bypasses it.
- Periodic access reviews that exclude service accounts, local accounts, or MSP identities.

Evidence package perspective

A strong evidence package links authorization, implementation, and verification. It can show the approved request, the resulting role or group membership, a current export of the affected population, the periodic review result, and an example of revocation. Evidence should also demonstrate how privileged provider access is limited and attributable.

Closure discipline matters. If the review identifies a gap in this family, the corrective record should identify the affected objective, owner, implementation change, validation method, evidence to retain, and any SSP or responsibility-matrix update. The assessment team should not close the finding merely because a configuration change was requested or a policy was rewritten.

Field Guide 2: Awareness and Training

Training should be assessed by comparing required populations with actual personnel who perform work in or around the assessed environment. The team should understand initial awareness, recurring training, role-specific training, handling guidance, and any specialized instruction needed for administrators, incident responders, or users of sensitive systems.

An MSP may train personnel on its own security program but still need customer-specific instruction for data handling, escalation, remote administration, or prohibited activities. Generic annual awareness training does not automatically cover those responsibilities.

Suggested assessment methods

Method	Readiness focus
Examine	Training policy and curriculum; required-role matrix; learning-management reports; new-hire records; overdue training reports; role-based training materials; acknowledgements for handling CUI; provider training commitments if relied upon.
Interview	HR or training coordinator; Harbor Point managers; NorthStar technicians with customer access; incident-response personnel; users who handle CUI. Ask when training is assigned, what triggers retraining, how missed training is escalated, and whether technicians understand customer-specific handling rules.
Test	Reconcile active user and privileged-access populations against training completion. Select recently hired or newly privileged individuals and verify that required training occurred before or within the approved timing. Confirm that overdue status triggers the defined response.

Common MSP/customer failure patterns

- Training reports exclude contractors or temporary staff.
- Privileged technicians receive the same curriculum as ordinary end users despite different responsibilities.
- Users complete training but customer-specific CUI handling instructions are absent.

- No process exists for overdue training or access suspension.
- Provider staff turnover is not reconciled to training and access populations.

Evidence package perspective

Evidence should identify the person, required course or instruction, completion date, role, and any follow-up. Where the MSP relies on centralized provider training, retain enough assurance to show that the personnel supporting the customer fall within the program.

Field Guide 3: Audit and Accountability

Audit readiness depends on complete and trustworthy event visibility. The team should know which systems generate relevant audit records, which events are enabled, where records are forwarded, how time and identity are preserved, who reviews activity, how privileged use is monitored, and how the organization reacts when a log source stops reporting.

Shared SIEM platforms can create attribution and privacy problems. Harbor Point evidence should identify the customer tenant or data partition and should not expose unrelated customers. Provider retention limits and service tiers must be reconciled with the customer’s logging design.

Suggested assessment methods

Method	Readiness focus
Examine	Logging standard; source inventory; SIEM or log-platform configuration; event-selection settings; retention configuration; alert rules; privileged-activity reports; log-source health dashboards; time synchronization settings; review tickets; incident links.
Interview	Beacon analysts; NorthStar engineers; system owners; incident responders; evidence custodians. Ask how new assets are added to logging, how failed collectors are detected, how retention is verified, and who can modify or delete audit information.
Test	Select in-scope assets and confirm that expected events reach the designated repository. Generate a safe test event and trace it from source to collection and review. Verify that one disabled or failed log source would be detected. Compare current source inventory to asset inventory.

Common MSP/customer failure patterns

- Important systems never onboarded to centralized logging.
- Collectors fail silently for weeks.
- Retention configured differently from the written plan.
- Privileged activity logged locally but not protected or reviewed.
- The customer cannot retrieve historical records without an individual provider engineer.

Evidence package perspective

A persuasive package combines a source inventory, configuration records, retention information, sample audit events, health monitoring, review tickets, and evidence of response to a logging failure.

Field Guide 4: Configuration Management

Configuration Management should show that the organization has defined secure states, controls change, limits unnecessary functionality, and detects or corrects drift. The gap assessment should trace a baseline from source to deployment and then trace representative changes from authorization through validation.

MSP automation creates leverage but also systemic risk. Global scripts, policies, and templates should be governed so that customer-specific requirements are not overwritten by generic defaults. Customer deviations should remain visible rather than becoming undocumented technician knowledge.

Suggested assessment methods

Method	Readiness focus
Examine	Configuration standards; endpoint and server baselines; network-device templates; cloud policies; change tickets; emergency-change records; software inventories; prohibited-software rules; automation scripts; exception records; drift reports.
Interview	Change manager; NorthStar engineering leads; endpoint administrators; network administrators; application owners. Ask who can modify baselines, how emergency changes are reviewed after the fact, how failed deployments are handled, and how customer-specific deviations are documented.
Test	Compare selected systems to the approved

	baseline. Review a recent standard change and an emergency change. Observe how a configuration policy is deployed and how exceptions appear in the management console. Confirm that unauthorized software or settings can be identified.

Common MSP/customer failure patterns

- Baselines exist only as PDFs and are not connected to deployed settings.
- Emergency changes never receive retrospective review.
- Technicians edit global scripts without change control.
- Software inventory differs materially from actual installations.
- Exceptions have no owner, reason, expiration, or compensating action.

Evidence package perspective

Evidence should show the approved baseline, deployed configuration, change record, success or failure results, exception handling, and periodic review. A before-and-after configuration export can be more persuasive than a narrative alone.

Field Guide 5: Identification and Authentication

Identification and Authentication requires the team to understand every identity class and authentication path. Workforce accounts, privileged identities, service accounts, devices, local accounts, application identities, automation credentials, API keys, and emergency credentials may all matter. The review should determine how uniqueness, authentication strength, credential lifecycle, and multifactor enforcement are implemented.

The MSP’s technician authentication system may be separate from the customer’s identity platform. The assessment should determine how provider identities are uniquely tied to people, how strong authentication is enforced, and how those identities map to customer-side activity.

Suggested assessment methods

Method	Readiness focus
Examine	Identity-provider policies; MFA configuration; password and authenticator settings; service-account inventory; local-account reports; privileged identities; recovery accounts; device identity controls; federation settings;

	authentication logs.
Interview	Identity administrators; service desk; application owners; NorthStar privileged technicians; security operations. Ask how exceptions are created, who can reset authenticators, how emergency credentials are protected, and which systems do not use the primary identity provider.
Test	Authenticate through representative standard, privileged, remote, and recovery paths. Confirm MFA or other required authentication controls. Verify that disabled identities cannot authenticate. Review local accounts on selected endpoints and servers.

Common MSP/customer failure patterns

- Break-glass or local accounts excluded from normal controls with no defined governance.
- Shared service accounts used interactively.
- MFA policy applies to cloud login but not RMM, VPN, or legacy administrative interfaces.
- Orphaned application credentials remain after personnel changes.
- Authentication logs cannot reliably identify the human behind provider activity.

Evidence package perspective

Combine identity exports, policy configuration, authentication logs, exception approvals, reset records, and representative tests. The strongest evidence shows both the policy and the observed enforcement.

Field Guide 6: Incident Response

Incident Response should be assessed as a coordinated operating process. The team needs to understand detection, triage, decision authority, containment, reporting, preservation, recovery, and post-incident improvement. Internal plans, MSP procedures, SOC escalation, contractual reporting, and customer management decisions must fit together.

Contracts often promise monitoring or incident support without defining containment authority or reporting responsibility. The assessment should distinguish detection, technical response, customer decision authority, and government or prime-contractor reporting duties.

Suggested assessment methods

Method	Readiness focus
Examine	Incident-response plan; contact lists; escalation procedures; SOC service description; recent incident tickets; tabletop records; preservation procedures; reporting decision records; lessons-learned actions; after-hours schedules.
Interview	Harbor Point incident coordinator; management; NorthStar on-call engineers; Beacon SOC; legal or contract personnel as appropriate. Ask who can isolate systems, who decides whether an event is an incident, how contractual reporting is triggered, and what happens when the primary contact is unreachable.
Test	Run a tabletop or controlled alert simulation. Confirm that contacts receive the notification, authority is clear, evidence is preserved, and decisions are recorded. Test one after-hours path and one provider-to-customer escalation.

Common MSP/customer failure patterns

- SOC sends alerts but no one is authorized to act.
- MSP isolates systems automatically even though the customer has not approved that authority—or the reverse, everyone waits for approval that was supposed to be delegated.
- Contact lists are outdated.
- Incident records do not preserve decision points or evidence custody.
- Tabletops never include providers or after-hours scenarios.

Evidence package perspective

Use plans, contact lists, service agreements, sample incidents, alert-to-ticket records, containment evidence, reporting decisions, preservation records, and exercise after-action reports.

Field Guide 7: Maintenance

Maintenance assessment should identify how systems are serviced, which tools are used, who is authorized, how remote maintenance is controlled, and how temporary or vendor access is ended. Routine support can mask maintenance activities that deserve explicit security treatment.

RMM makes maintenance efficient but may create persistent access. The customer should understand how the MSP restricts maintenance privileges, monitors use, separates tenants, and responds when technician employment or role changes.

Suggested assessment methods

Method	Readiness focus
Examine	Maintenance procedures; vendor-support agreements; remote-maintenance logs; temporary-account records; diagnostic tools; device repair or return records; authorization records; sanitization evidence when applicable.
Interview	NorthStar support technicians; system administrators; vendor coordinators; asset custodians. Ask how third-party support sessions are approved, whether vendors receive standing access, and what happens to devices sent outside the controlled location.
Test	Observe an approved remote-maintenance session or review a recent session end to end. Confirm authentication, attribution, authorization, termination, and records. Verify that temporary accounts or tools are removed when work is complete.

Common MSP/customer failure patterns

- Vendor support accounts remain enabled indefinitely.
- Remote sessions are not attributable to individual technicians.
- Temporary maintenance tools remain installed.
- Devices leave the facility without an approved handling process.
- Maintenance records show completion but not customer authorization or validation.

Evidence package perspective

Representative maintenance tickets, session logs, authorization, tool records, temporary-account lifecycle, and device handling records can support the internal conclusion.

Field Guide 8: Media Protection

Media Protection should begin with actual information movement. Identify removable storage, printed CUI, exported reports, backup media, mobile devices, replacement drives, and other media that can contain protected information. Then evaluate access, transport, marking where applicable, storage, sanitization, and destruction.

Provider technicians may create temporary exports, diagnostic bundles, screenshots, or backup copies during support. Those artifacts can become media or data-handling issues even if the customer normally works in cloud applications.

Suggested assessment methods

Method	Readiness focus
Examine	Media policy; removable-media settings; encryption configuration; media inventories; destruction certificates; print rules; backup-media procedures; device disposal records; export restrictions.
Interview	Users who handle engineering information; IT asset staff; NorthStar support; records or facilities personnel. Ask what happens when users need to move files, print drawings, replace failed drives, or return leased equipment.
Test	Check representative endpoints for removable-media restrictions. Review disposal of a recent storage device. Verify that an approved encrypted device is handled according to procedure. Observe how printed sensitive material is stored or destroyed.

Common MSP/customer failure patterns

- USB use restricted by policy but not technically enforced.
- Support screenshots or exports stored in uncontrolled ticket attachments.
- Failed drives returned to vendors without an approved sanitization path.
- Printed CUI left in shared spaces.
- Destruction evidence cannot be tied to the specific media or asset.

Evidence package perspective

Evidence can include device-control configuration, media inventories, approved exceptions, encryption status, destruction records, and controlled examples of printed or exported information handling.

Field Guide 9: Personnel Security

Personnel Security should connect employment and role decisions to security actions. Screening, hiring, transfer, termination, sanctions, and changes in duties should trigger predictable updates to logical and physical access. The assessment should test the workflow, not just the HR policy.

Customer risk can persist when an MSP removes a technician from its workforce but customer-specific groups, shared vault permissions, or local credentials remain. Provider offboarding should therefore be reconciled to customer access paths.

Suggested assessment methods

Method	Readiness focus
Examine	Personnel-security policy; screening records or assurance statements; onboarding and termination procedures; HR-to-IT notifications; access-removal tickets; provider personnel practices; sanctions records where applicable.
Interview	HR; managers; service desk; physical-security personnel; NorthStar management. Ask how urgent terminations are handled, how provider technician changes reach customer access systems, and how role transfers differ from new hires.
Test	Select recent hires, transfers, and terminations. Trace each event from personnel decision to account, badge, group, remote-support, and application access changes. Confirm completion and timing.

Common MSP/customer failure patterns

- Termination process removes primary accounts but misses local or application identities.
- Provider technician changes rely on manual memory.
- Role transfers accumulate privileges.
- HR and IT timestamps cannot be correlated.

- Physical access remains after logical access is removed, or vice versa.

Evidence package perspective

Event-based personnel samples are strong: HR notice, approved role, provisioning or revocation tickets, identity exports, badge records, and verification that access changed as intended.

Field Guide 10: Physical Protection

Physical Protection requires the team to identify where systems and information exist physically and who can enter those locations. Customer offices, server rooms, storage areas, alternate work sites, provider facilities, and cloud facilities may involve different responsibilities and evidence.

Do not confuse a provider's protected data center with the customer's full physical responsibility. Laptops, printed drawings, networking equipment, and local server rooms remain customer-side issues even when major applications are hosted elsewhere.

Suggested assessment methods

Method	Readiness focus
Examine	Physical-access policy; authorized-person lists; badge or key records; visitor logs; facility diagrams; server-room controls; alternate-work-site rules; provider facility assurance; device storage procedures.
Interview	Facilities personnel; office managers; remote workers; IT staff; provider representatives. Ask how visitors are escorted, how lost badges are handled, how after-hours entry is reviewed, and how remote workers secure devices and printed material.
Test	Observe facility entry controls and server-room access. Select a recent visitor or badge-change record. Verify that remote-work requirements are practical and understood. Confirm that terminated personnel no longer have physical access.

Common MSP/customer failure patterns

- Visitor logs exist but are not reviewed or attributable.
- Shared keys cannot be tied to individuals.

- Server rooms double as general storage with uncontrolled access.
- Remote-work rules exist but users cannot explain secure storage expectations.
- Provider physical assurances are cited for assets that are actually at the customer site.

Evidence package perspective

Use access lists, visitor records, badge changes, facility observations, remote-work acknowledgements, and provider assurance appropriate to the actual service boundary.

Field Guide 11: Risk Assessment

Risk Assessment should demonstrate both periodic organizational risk evaluation and a functioning vulnerability-management process. For vulnerability scanning, the team should understand scope, frequency, authentication, applications, excluded assets, newly identified vulnerabilities, remediation, exception decisions, and rescanning.

A managed scanning service may provide reports without owning remediation. The responsibility matrix should show who evaluates findings, who schedules fixes, who accepts risk, and who verifies closure.

Suggested assessment methods

Method	Readiness focus
Examine	Risk assessments; vulnerability-scanning procedures; asset coverage reports; scanner configuration; credentialed-scan status; vulnerability results; remediation tickets; exception approvals; rescans; management review.
Interview	Security lead; NorthStar vulnerability team; asset owners; application owners; management. Ask how scan scope is derived, how new assets are added, how failures are detected, who accepts exceptions, and how application vulnerabilities are handled.
Test	Reconcile scanner targets to the asset inventory. Review failed or unauthenticated scans. Trace selected findings from discovery through remediation and rescan. Confirm that newly identified significant vulnerabilities trigger the defined process.

Common MSP/customer failure patterns

- High scan percentages conceal missing critical assets.
- Credentialed scans fail but reports are still accepted.
- Applications are excluded from vulnerability review.
- Tickets close when patches are deployed rather than when rescans confirm correction.
- Exceptions have no expiration or management decision.

Evidence package perspective

Coverage reconciliation, scan configuration, representative results, remediation records, exception decisions, and successful rescans provide a coherent evidence chain.

Field Guide 12: Security Assessment

Security Assessment is the governance family that asks whether the organization evaluates controls, manages corrective actions, monitors security, and keeps the SSP current. The gap assessment itself can contribute evidence, but the organization should also show how assessment and monitoring occur over time.

An MSP can generate technical monitoring data, but the customer retains governance responsibilities unless explicitly and validly allocated. The assessment should not confuse service reports with the customer's broader control-assessment and SSP-maintenance obligations.

Suggested assessment methods

Method	Readiness focus
Examine	Prior internal assessments; government or third-party assessment results if applicable; POA&Ms or remediation registers; continuous-monitoring records; SSP revision history; management review minutes; closed-finding validation.
Interview	SSP owner; security manager; management; control owners; remediation coordinators. Ask how findings become projects, how closure is verified, how recurring monitoring is selected, and how system changes trigger SSP updates.
Test	Select closed findings and verify that corrective evidence exists. Compare the SSP to current architecture and responsibility records. Review whether planned monitoring activities actually

	occurred.

Common MSP/customer failure patterns

- Findings close based on owner assertion with no re-test.
- SSP describes retired services.
- Monitoring reports are produced but never reviewed.
- POA&M items have dates but no dependency or validation plan.
- Repeated gaps indicate that root causes are not addressed.

Evidence package perspective

Assessment reports, remediation records, re-test results, SSP revision records, monitoring evidence, and management decisions should form a continuous improvement trail.

Field Guide 13: System and Communications Protection

This family should be assessed through architecture and live configuration together. Boundary protection, communication paths, remote connections, encryption, key and certificate management, session protections, collaborative devices, and separation mechanisms can be misunderstood when diagrams lag behind implementation.

Administrative tunnels and remote-support channels are often separate from business-user paths. The customer should understand those channels, their authentication, encryption, logging, and failure modes. Shared provider infrastructure must be evaluated through the service boundary actually used.

Suggested assessment methods

Method	Readiness focus
Examine	Network and data-flow diagrams; firewall and security-group configuration; VPN settings; remote-access architecture; encryption configuration; certificate and key inventories; collaboration-device controls; DNS and email security configuration; cloud network controls.
Interview	Network engineers; cloud administrators; NorthStar remote-support engineers; security architects; application owners. Ask which paths can reach CUI systems, who approves new connections, how encryption choices are made, and how keys or certificates are renewed and

	revoked.
Test	Trace representative network paths. Verify boundary rules and remote-access controls. Observe encryption for selected communications. Review one certificate or key lifecycle. Confirm that diagrams match actual routes and cloud configuration.

Common MSP/customer failure patterns

- Diagrams omit cloud peering, vendor tunnels, or MSP remote channels.
- Firewall rules permit broader access than the documented design.
- Certificates expire unexpectedly because ownership is unclear.
- Encryption is assumed from the product name but not verified for the selected protocol or path.
- Collaborative devices introduce uncontrolled microphones, cameras, or file transfer.

Evidence package perspective

Current diagrams, configuration exports, approved connection records, encryption settings, certificate inventories, and representative path tests support the security story.

Field Guide 14: System and Information Integrity

System and Information Integrity should show how the organization detects and corrects flaws, protects against malicious code, receives and evaluates advisories, monitors system integrity, and responds to suspicious conditions. Asset coverage is essential because a strong protection stack is irrelevant to systems that are missing from it.

Managed patching and endpoint protection often span multiple tools. The assessment should determine whether exclusions, failed deployments, reboot deferrals, and unsupported systems remain visible and whether responsibility for those conditions is clear.

Suggested assessment methods

Method	Readiness focus
Examine	Patch policy and deployment reports; EDR or antimalware coverage; agent-health dashboards;

	exclusion records; security-advisory process; remediation tickets; vulnerability links; unauthorized-use alerts; exception approvals.
Interview	Endpoint team; server administrators; security operations; NorthStar patching staff; application owners. Ask how unhealthy agents are detected, how emergency patches are handled, who approves exclusions, and how advisories are mapped to affected systems.
Test	Reconcile in-scope assets to active protection. Select recent patches and verify deployment and validation. Review unhealthy or excluded agents. Trace a security advisory from receipt through applicability decision and corrective action.

Common MSP/customer failure patterns

- Dashboard percentages hide missing high-value systems.
- Patch jobs report success even though devices never rebooted into the corrected state.
- EDR exclusions are broad and undocumented.
- Advisories are received but not mapped to customer assets.
- Unsupported appliances fall outside normal patch processes with no alternative treatment.

Evidence package perspective

Asset-to-agent reconciliation, patch records, health reports, exclusion approvals, advisory decisions, remediation tickets, and follow-up validation create a defensible evidence chain.

Field Guide Wrap-Up: Cross-Family Consistency Checks

After completing the family reviews, perform cross-family checks. CMMC requirements do not operate in isolation. A personnel termination affects Personnel Security, Access Control, Identification and Authentication, Physical Protection, and potentially Audit and Accountability. A new remote-management platform affects scope, Access Control, Identification and Authentication, Maintenance, Audit, Configuration Management, and System and Communications Protection. Reviewing only family-by-family can miss these dependencies.

- Reconcile the asset inventory against EDR, vulnerability scanning, logging, backup, patching, and configuration-management populations.
- Reconcile workforce and provider personnel against identity, privileged access, MFA, training, physical access, and termination records.
- Reconcile network diagrams against firewall rules, remote-access tools, cloud integrations, provider connections, and actual observed paths.
- Reconcile incident-response contacts against SOC routing, MSP on-call schedules, customer decision authority, and contractual reporting responsibilities.
- Reconcile SSP statements against the responsibility matrix, provider CRMs, service agreements, procedures, and current configuration.
- Reconcile closed remediation items against re-test evidence rather than ticket status alone.

These cross-checks often produce the highest-value readiness findings because they compare systems that different teams maintain. A customer may have accurate records inside each department and still have a control failure at the boundary between those records. The MSP is often well positioned to expose those boundary conditions because its service platform sees identity, endpoint, network, ticket, monitoring, and backup activity together. That visibility should be used carefully and documented rather than converted into unsupported assumptions.

Review Questions

1. What is the purpose of establishing a dated assessment baseline before evaluating individual requirements?

2. Why can an internal readiness review not be represented as a certification decision?

3. How do examine, interview, and test methods complement one another?

4. Why should a requirement be decomposed into its assessment objectives?

5. What is the difference between an implementation gap and an evidence gap?

6. How should the team treat an unresolved provider dependency?

7. Why is a product name insufficient evidence of control implementation?

8. What characteristics make evidence more persuasive and useful?

9. Why should interviews follow real events and workflows rather than requirement vocabulary alone?

10. What should a safe technical test define before execution?

11. How should a strong finding describe scope and corrective ownership?

12. What cross-cutting issues make Access Control and Identification and Authentication especially important for MSPs?

13. How can log-source coverage fail even when a SIEM is deployed?

14. Why should vulnerability scanning be reconciled to the asset inventory?

15. What should be reviewed when an MSP uses shared administrative platforms?

16. Why must cloud services be evaluated at the offering and tenant level?

17. What is the difference between an internal readiness metric and an official CMMC score?

18. Why does a POA&M not make an unmet requirement implemented?

19. What factors should influence remediation sequencing?

20. What evidence is needed to close a corrective action reliably?

21. How did the Harbor Point case study distinguish confirmed gaps from pending provider evidence?

22. Why should remediation findings trigger SSP and responsibility-matrix reconciliation?

23. What is the purpose of a validation workshop?

24. How can an organization sustain readiness after the gap assessment ends?

Answer Guidance

Questions 1 through 4 focus on assessment discipline. A conclusion has meaning only when the team can identify the environment, requirement source, objective, evidence, and time period to which it applies. Internal work can support readiness but cannot substitute for an authorized certification process.

Questions 5 through 11 focus on finding quality. Preserve the difference between implementation, evidence, documentation, scope, and provider issues. Use examine, interview, and test methods as needed. State what an artifact proves and what it does

not prove. Write findings so that another person can understand the affected workflow and validate the correction.

Questions 12 through 16 focus on technical and provider dependencies. Administrative platforms, cloud services, identity systems, monitoring, vulnerability management, and remote access should be evaluated through actual configuration, service boundaries, customer responsibilities, and retrievable evidence rather than vendor reputation.

Questions 17 through 24 focus on remediation and sustainment. Internal metrics should drive work without masquerading as official scores. Planned actions are not completed controls. Closure requires re-testing, document reconciliation, management awareness, and a process that remains operational after the readiness project ends.

Key Terms

Term	Meaning in this chapter
Assessment baseline	The dated scope, architecture, responsibility, source, and evidence context used for the internal review.
Assessment objective	A determination identified in the applicable assessment procedure that helps evaluate a security requirement.
Examine	Review of documents, records, configurations, outputs, and other assessment objects.
Interview	Discussion with personnel to determine how responsibilities and processes are understood and performed.
Test	Exercise or observation of a mechanism or process to determine how it operates.
Implementation gap	A required safeguard or activity that is absent or materially incomplete.
Evidence gap	Insufficient support to substantiate an implementation claim even when the control may exist.
Documentation gap	Conflict or incompleteness in the SSP, procedure, inventory, diagram, or other controlled record.
Provider dependency	A conclusion that depends on an external service capability, responsibility, or evidence source.
Re-testing	Evaluation performed after remediation to determine whether the intended corrective result has been achieved.
Root cause	The underlying process, design, governance, or technical condition that produced a finding.
Remediation wave	An internal grouping of corrective work for practical sequencing; not an official CMMC category.
Evidence custodian	The role responsible for controlled preservation and

	authorized retrieval of supporting records.
Internal readiness conclusion	An organization's own assessment result used for preparation and improvement, not a certification decision.

Closing Perspective

The gap assessment is where CMMC readiness becomes concrete. Scope, responsibilities, policies, tools, and procedures must converge into an implementation that people can explain and evidence can support. The exercise is valuable precisely because it exposes disagreements before they become external findings or operational incidents.

For the MSP, the strongest readiness service is not the one with the largest spreadsheet. It is the one that helps the customer understand the real environment, makes responsibilities executable, tests the implementation honestly, preserves uncertainty where facts are missing, and converts findings into corrections that can be verified. That discipline is useful whether the next milestone is a self-assessment, a government review, an eventual certification requirement, or simply the customer's obligation to protect sensitive information.

Harbor Point's progress across Chapters 5 through 7 illustrates the sequence. First define the environment. Then define who does the work. Then determine whether the work, evidence, and documentation actually satisfy the applicable requirements. The next stage is to turn the confirmed gaps into a managed remediation program that can be sustained through change.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. Use the current edition and applicable provisions for scope, assessment, POA&M, affirmation, and external service providers.

R2. National Institute of Standards and Technology. NIST SP 800-171A, June 2018, Assessing Security Requirements for Controlled Unclassified Information. Used here for the Revision 2 assessment objectives and examine, interview, and test methods incorporated into the referenced Level 2 framework.

R3. National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and

Organizations. The 110-requirement baseline referenced by the published CMMC Level 2 framework discussed in this chapter.

R4. Department of Defense / Office of Industrial Base Growth. July 13, 2026 announcement suspending CMMC Phase II requirements while maintaining Phase I self-assessment requirements and continuing underlying safeguarding obligations.

R5. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Review the current clause and the customer’s actual contract for applicable safeguarding, reporting, preservation, cloud, and flow-down obligations.

R6. Department CMMC resources and FAQs. Use current official program guidance to confirm acquisition implementation status, assessment pathways, and documentation.

Sources reviewed September 19, 2026. This chapter is educational and operational guidance for readiness work. It does not replace the governing regulation, the applicable solicitation or contract, legal advice, or an authorized CMMC assessment.

CMMC for MSPs

From Readiness to Certification

Chapter 8

Building the CMMC Remediation Roadmap

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and source context

8.1–8.8 Turning findings into a managed remediation program

8.9–8.15 Prioritization, dependencies, ownership, and governance

8.16–8.22 Technical remediation patterns for MSP environments

8.23–8.29 Evidence, documentation, provider, and contract corrections

8.30–8.35 POA&M discipline, validation, change control, and closure

8.36–8.39 Budgeting, resourcing, metrics, and executive decisions

8.40–8.43 Harbor Point remediation case study and roadmap workshop

Remediation field guide, review questions, key terms, and official references

Chapter Purpose

Chapter 7 identified the gap. Chapter 8 decides what the organization will do about it. That sounds simple until the findings compete for the same engineers, budget, maintenance windows, customer approvals, provider changes, and management attention. A remediation roadmap is therefore not a list of open tickets. It is the controlled plan that converts verified weaknesses into implemented, tested, documented, and sustainable security outcomes.

For an MSP, remediation is rarely confined to one organization. Harbor Point may own the business decision, NorthStar may perform the technical work, Beacon may need to modify alerting, a cloud provider may need to expose evidence or enable a feature, and a software vendor may need to support a configuration change. The roadmap must make these dependencies visible before dates are promised. Otherwise the plan becomes an optimistic calendar rather than an executable security program.

This chapter continues the Harbor Point Engineering case study. We will take the confirmed findings from the gap assessment and turn them into work packages, remediation waves, validation plans, documentation changes, provider actions, and management decisions. The objective is not simply to make findings disappear from a dashboard. The objective is to correct the condition that produced the finding, prove that the correction works, and leave the organization with a process that can continue operating after the immediate readiness effort ends.

The chapter also distinguishes internal corrective-action tracking from formal CMMC POA&M treatment. Internal teams should track every relevant weakness. Formal eligibility, scoring, time limits, and closure conditions must follow the applicable rule and current official guidance. A roadmap can organize work, but it cannot waive a requirement or convert planned work into completed implementation.

Learning Objectives

- Convert gap-assessment findings into specific remediation work packages with defined outcomes, owners, dependencies, validation, and evidence.
- Prioritize remediation using security significance, scope, dependency, effort, contractual timing, and operational risk rather than simple requirement order.
- Distinguish immediate containment, durable remediation, compensating operational actions, and long-term architectural change.

- Build remediation waves that coordinate identity, endpoint, network, cloud, logging, incident response, provider, policy, and evidence work.
- Understand the difference between an internal corrective-action register and formal CMMC POA&M treatment.
- Integrate change management, rollback, testing, documentation, and evidence capture into remediation execution.
- Budget and resource remediation without hiding provider costs, licensing changes, labor, downtime, training, or sustainment effort.
- Measure progress using closure quality and risk reduction rather than ticket counts alone.
- Prepare management to make explicit decisions when remediation requires scope reduction, architecture redesign, contract change, or acceptance of business disruption.

Source and Applicability Note

This chapter uses the published CMMC framework in 32 CFR Part 170 and the Level 2 baseline based on NIST SP 800-171 Revision 2. Formal POA&M eligibility and assessment consequences must be determined from the applicable CMMC rule, contract, solicitation, and official program guidance. Internal corrective-action planning can be broader than formal POA&M treatment because an organization should manage all known weaknesses, even when a particular item cannot be carried as an allowable formal POA&M. [R1, R2]

On July 13, 2026, the Department announced the immediate suspension of CMMC Phase II requirements while Phase I self-assessment requirements remain in place and the Department conducts a broader program review. The announcement also emphasized that contractors and subcontractors remain obligated to safeguard covered defense information under applicable contractual requirements. Remediation therefore remains operationally important even while acquisition implementation is under review. [R3]

The prioritization models, wave structures, severity labels, project templates, and management dashboards in this chapter are teaching and management methods. They are not official CMMC scoring categories unless specifically identified as such from an authoritative source.

8.1 A Finding Is Not Yet a Remediation Plan

A gap finding tells the organization what is wrong or unsupported. It does not necessarily tell the organization how to fix it. The remediation team must translate the condition into an intended security outcome, determine the root cause, identify affected assets and workflows, and choose a correction that fits the actual architecture. A weak plan simply repeats the finding as a task: fix MFA, improve logging, update policy. A strong plan defines what will change and how the team will know the intended result has been achieved.

Harbor Point begins each work package with five questions. What condition must no longer be true? What secure condition must become true? Which systems, users, providers, and documents are affected? What dependencies must be satisfied first? What evidence will prove closure? These questions force the plan away from activity and toward outcome.

The distinction is important because many remediation projects generate visible activity without reducing the original risk. A patch deployment can finish while vulnerable systems remain. A policy can be signed while technicians continue using the old process. A new MFA product can be purchased while administrative paths remain outside it. Closure must therefore be tied to the corrected condition, not the amount of work performed.

Working rule: Remediation is complete only when the intended control outcome has been implemented, verified, and reconciled with the security documentation.

8.2 Preserve the Original Finding and Its Evidence

Do not rewrite history when remediation begins. The original finding, evidence, affected objective, scope, and internal conclusion should remain preserved. Corrective work should be linked to that record rather than replacing it. This gives the organization a defensible trail from observed weakness to implemented correction.

Harbor Point assigns each finding a stable identifier. The remediation record references that identifier, records the root cause and corrective design, and then adds implementation and validation evidence. If the finding is later narrowed because better information becomes available, the original observation remains visible together with the reason for the change.

This practice prevents a common readiness failure in which a spreadsheet row changes from red to green but nobody can explain what changed, when it changed,

who validated it, or whether the original evidence was misunderstood. A remediation history should make improvement easier to audit rather than easier to forget.

8.3 Separate Containment, Correction, and Prevention

Some findings create immediate exposure. The organization may need to contain the condition before the durable remediation is ready. If an unauthorized remote access path exists, Harbor Point may disable it now, then redesign the approved remote administration model later. If a vulnerable service cannot be patched immediately, the team may restrict access, increase monitoring, or remove the service from use while a permanent solution is developed.

Containment reduces immediate risk. Correction fixes the identified condition. Prevention addresses the process or architecture that allowed the condition to appear or recur. These three layers should not be confused. Removing one former technician from an access group corrects that account. Improving provider offboarding prevents the same problem from recurring. Reviewing all provider groups addresses the possibility that the condition exists elsewhere.

A remediation roadmap should state which layer each task addresses. Management may approve temporary containment while scheduling durable work, but the temporary step should not be reported as permanent closure unless it truly satisfies the applicable requirement and intended operating model.

Layer	Purpose	Example
Containment	Reduce immediate exposure	Disable an uncontrolled administrative path
Correction	Fix the verified condition	Require approved MFA on the administrative path
Prevention	Reduce recurrence	Add access-path review to service onboarding and change control

8.4 Find the Root Cause Before Scaling the Fix

Root cause analysis does not need to become a lengthy forensic exercise for every minor documentation defect. It should be proportional to the likelihood of recurrence and the impact of the condition. Repeated or cross-cutting findings deserve deeper analysis because the visible symptom may be only one example of a larger failure.

Harbor Point finds two unmanaged endpoint agents. The obvious correction is to reinstall the agent. The deeper question is why rebuilt systems were not automatically enrolled. The answer reveals an outdated deployment image and a missing reconciliation step between asset inventory and the endpoint-protection console. Fixing the image and reconciliation process prevents future rebuilt systems from silently losing coverage.

Useful root-cause categories include governance, architecture, process design, responsibility ambiguity, configuration error, automation defect, training, provider limitation, insufficient licensing, missing monitoring, and uncontrolled exception handling. The category is not the solution by itself; it helps the team design work that addresses the source rather than only the symptom.

8.5 Convert Findings into Work Packages

A work package is the smallest unit of remediation that management can assign, fund, implement, and validate coherently. It may contain several technical tasks when those tasks share one outcome. For example, closing a privileged-access gap may require identity-group cleanup, MFA policy changes, RMM role changes, local account handling, procedure updates, and an access-review record. Splitting those tasks among separate tickets without a controlling work package makes it difficult to know whether the complete security outcome was achieved.

Each work package should identify the finding or findings addressed, intended outcome, scope, owner, contributors, technical steps, provider actions, prerequisites, change window, rollback, validation, evidence, documentation updates, residual risks, and closure authority. The level of detail should match the complexity of the change.

NorthStar uses project tickets for execution but keeps the remediation work package as the authoritative record. Tickets may be reopened, reassigned, or split. The work package preserves the complete outcome and connects the individual tasks back to the original gap.

Work package field	**Purpose**
Finding linkage	Preserves why the work exists
Target state	Defines the secure outcome
Scope	Identifies affected assets, users, services, and locations
Owner and contributors	Assigns decision and execution responsibility
Dependencies	Identifies prerequisites and external actions
Validation	Defines how completion will be tested
Evidence	Defines what records demonstrate closure

Documentation updates	Identifies SSP, matrix, procedure, diagram, or inventory changes

8.6 Do Not Let the Remediation Register Become Another Inventory

A remediation register should drive decisions and execution. It should not become a passive list containing dozens of stale rows with no owner, no validation plan, and dates that are repeatedly pushed forward. Every open item should have a meaningful next action and an accountable role.

Harbor Point distinguishes backlog from active remediation. Backlog means the issue is known but has not yet entered an approved work window. Active means resources are assigned and dependencies are being executed. Blocked means a specific unresolved dependency is preventing progress. Validation means implementation is complete but closure evidence is still being tested. Closed means the defined outcome has been verified.

These states help management see why work is not moving. A blocked item should name the dependency. Waiting on vendor is insufficient. Waiting on provider tenant-retention export requested September 10, required to validate AU evidence, is actionable. Precision makes escalation possible.

8.7 Group Related Findings Before You Fix Them One by One

Gap assessments often produce many findings that share one cause. Separate rows may identify stale privileged access, inconsistent local administrator use, weak service-account governance, and MFA exceptions. Treating each as an isolated ticket can produce a patchwork of fixes while the identity architecture remains fragmented.

Before sequencing work, Harbor Point clusters findings by system and dependency. Identity findings become an identity-hardening program. Endpoint findings become a coverage and baseline program. Logging findings become a telemetry and retention program. Incident findings become an escalation and authority program. Documentation findings are linked to the technical programs they describe.

Clustering also helps budget. One licensing change may resolve several findings. One architecture decision may eliminate multiple unmanaged paths. One provider contract change may make evidence available across several objectives. Remediation should

look for these leverage points without assuming that one change automatically satisfies every related requirement.

8.8 Define the Target Architecture Before Buying Tools

A remediation roadmap frequently reveals pressure to purchase products. The team should resist tool-first decisions until it can explain the target architecture and operating model. A new tool adds identities, integrations, logs, support responsibilities, evidence, licensing, and failure modes. It can reduce complexity only when the design intentionally replaces or consolidates existing capability.

Harbor Point's privileged-access findings could be addressed by buying a dedicated PAM platform, redesigning existing identity and RMM controls, or reducing administrative paths. The correct decision depends on the environment, risk, resources, contractual obligations, and sustainment capability. The roadmap should compare these options against the desired control outcome.

A remediation design should also consider scope impact. Moving CUI into a more isolated enclave may reduce complexity. Adding a broadly connected management platform may expand dependencies. Every major architecture change should trigger a scoping review before implementation, not after the project is complete.

8.9 Prioritize by Security Significance, Not by Convenience

Easy findings are tempting because they create rapid dashboard improvement. That can be useful for momentum, but remediation sequencing should first consider security significance. An uncontrolled privileged access path deserves attention even if the procedure-formatting findings are easier to close.

Harbor Point uses a management priority model that considers impact, exposure, breadth, dependency, exploitability or misuse potential, contractual timing, and feasibility. The model does not create an official CMMC score. It gives executives a repeatable way to compare work that competes for the same resources.

Priority should be reviewed after dependencies are understood. A technically severe issue that requires a six-month platform migration may need immediate containment and a long-term project, while another high-impact issue can be corrected in days. The roadmap should show both paths rather than forcing every finding into one linear queue.

Factor	Question

Security impact	What could an attacker or unauthorized user do if the condition remains?
Exposure	How reachable or frequently used is the affected path?
Breadth	How many assets, users, locations, or workflows are affected?
Dependency	Which other controls depend on this correction?
Timing	Is there a contract, operational, or assessment milestone?
Feasibility	Can the condition be contained or corrected safely with available resources?

8.10 Build Remediation Waves Instead of One Giant Deadline

A roadmap should organize work into manageable waves. A wave groups corrections that share dependencies, teams, or change windows. It gives management a meaningful milestone while avoiding the fiction that every finding will close on one date.

Wave One at Harbor Point addresses immediate privileged access, unmanaged security agents, critical log-source failures, and incident escalation ambiguity. Wave Two addresses foundational architecture, baseline configuration, vulnerability coverage, backup validation, and provider evidence. Wave Three addresses documentation reconciliation, automation, evidence retrieval, metrics, training, and sustainment improvements.

Wave placement is not a statement that later items are unimportant. It is an execution decision. Every deferred condition should remain visible with interim risk treatment where appropriate. The roadmap should identify which later work cannot begin until earlier dependencies are satisfied.

8.11 Map Dependencies Explicitly

Many remediation failures are scheduling failures disguised as technical failures. A team promises an MFA rollout before it has identified all authentication paths. It schedules a SIEM migration before applications can generate the required events. It rewrites the SSP before the architecture decision has been made. Dependencies should therefore be recorded as first-class roadmap data.

Dependency types include technical prerequisites, provider changes, procurement, licensing, contract amendments, maintenance windows, application compatibility, user training, management approval, data migration, and staffing. A task can have

more than one dependency and those dependencies may belong to different organizations.

Harbor Point uses dependency reviews at each roadmap meeting. If a task slips, the team asks which downstream items are affected. This prevents hidden cascade effects and helps management decide whether to add resources, change sequence, or choose another technical design.

8.12 Assign One Outcome Owner Even When Many Teams Contribute

Shared responsibility is normal; shared accountability is dangerous. Each remediation work package should have one outcome owner who is responsible for carrying the work to validated closure. That person may not perform every task, but they coordinate dependencies and ensure that the final state is demonstrated.

For Harbor Point's incident escalation correction, the customer security coordinator owns the outcome because the customer retains decision authority. NorthStar updates on-call routing and technical procedures. Beacon updates notification logic. The customer contract manager reconciles service language. The single outcome owner confirms that these pieces create one coherent process and that the tabletop exercise validates it.

The owner should have enough authority to escalate blockers. Assigning a technician as owner of a remediation that requires contract amendment and executive approval creates a structural delay. Ownership should match the decisions needed to close the work.

8.13 Separate Decision Authority from Technical Execution

Chapter 6 distinguished who decides from who executes. Remediation should preserve that distinction. A NorthStar engineer can configure a security policy, but Harbor Point may need to approve the user impact, maintenance window, exception policy, or business risk. A provider can recommend an architecture, but the customer may own the decision to change how CUI is handled.

Work packages should therefore identify decision points, not just task assignees. Where the roadmap depends on a customer choice, the decision should have a due date and consequences. Otherwise technical teams can appear late when they are actually waiting for authority.

Explicit decision records also strengthen evidence. They show that important exceptions, scope changes, and risk treatments were not informal technician choices. The record should state what was decided, by whom, based on what information, and which implementation actions follow.

8.14 Plan for User and Business Disruption

Security remediation changes how people work. Stronger authentication can affect service accounts and automation. Network segmentation can break legacy discovery. Session timeouts can interrupt engineering tools. Application hardening can disable macros or integrations. A roadmap that ignores operational impact encourages emergency exceptions after deployment.

Harbor Point includes business testing, communication, training, and rollback in major work packages. Application owners validate critical workflows before production enforcement. NorthStar pilots policies on representative systems. Exceptions discovered during the pilot are treated as design inputs, not as reasons to abandon the control.

User disruption should be managed, but it should not be used as an undefined veto. Management needs a clear choice: accept a controlled implementation plan, redesign the business process, isolate the legacy dependency, or determine another compliant path. Keeping the issue explicit is better than leaving a weak control in place indefinitely.

8.15 Protect the Environment While Remediation Is Underway

Some corrections take months. The organization still needs to manage risk during the project. Interim protections may include disabling unnecessary access, restricting network routes, increasing monitoring, shortening credential lifetime, adding manual review, reducing data exposure, isolating unsupported systems, or limiting the affected business process.

These measures should be documented as interim risk treatments, not silently described as permanent compliance. The team should identify the condition they reduce, their limitations, owner, start date, review trigger, and end condition. Interim measures that become permanent through neglect are a common source of technical debt.

The remediation register should therefore track both the durable work and the temporary protection. Closure occurs only when the final target state is validated or when management has formally changed the architecture or business process in a way that resolves the original requirement.

8.16 Identity and Privileged Access Remediation

Identity remediation should begin with the authoritative population: employees, contractors, provider technicians, service identities, devices, local accounts, application roles, emergency credentials, and automation. Reconcile these populations before changing policies so the team understands who and what will be affected.

Common work packages include removing stale access, redesigning privileged groups, enforcing approved MFA paths, reducing local administrators, governing emergency accounts, rotating exposed credentials, improving service-account ownership, and creating recurring access reviews. The validation plan should test both authorized access and denied access.

For identity and privileged access remediation, Harbor Point also identifies documentation and evidence consequences. Any change that affects scope, responsibility, configuration, operating procedure, or provider dependency triggers updates to the relevant SSP sections, diagrams, inventories, and evidence index. This keeps remediation from creating a technically improved but inaccurately documented environment.

8.17 Endpoint Coverage and Secure Baseline Remediation

Endpoint findings often combine missing agents, inconsistent baselines, patch failures, unsupported systems, and uncontrolled local settings. Start by reconciling the in-scope inventory against EDR, patching, vulnerability, logging, encryption, and configuration-management consoles.

The durable correction is a lifecycle process: new systems enroll automatically, rebuilds return to the baseline, unhealthy agents are detected, exceptions are approved and time-limited, and decommissioned assets leave all management systems. Reconciliation metrics should continue after the project closes.

For endpoint coverage and secure baseline remediation, Harbor Point also identifies documentation and evidence consequences. Any change that affects scope,

responsibility, configuration, operating procedure, or provider dependency triggers updates to the relevant SSP sections, diagrams, inventories, and evidence index. This keeps remediation from creating a technically improved but inaccurately documented environment.

8.18 Logging, Monitoring, and Audit Remediation

Logging remediation should identify required sources, events, retention, protection, review, alerting, and health monitoring. Adding one more log collector does not fix a design in which important systems are absent or no one responds when feeds stop.

A strong work package maps assets to expected telemetry, enables required audit settings, centralizes or protects records as appropriate, verifies time consistency, detects source failures, and defines review and escalation. Provider retention and export limitations should be addressed contractually or architecturally.

For logging, monitoring, and audit remediation, Harbor Point also identifies documentation and evidence consequences. Any change that affects scope, responsibility, configuration, operating procedure, or provider dependency triggers updates to the relevant SSP sections, diagrams, inventories, and evidence index. This keeps remediation from creating a technically improved but inaccurately documented environment.

8.19 Network Boundary and Remote Access Remediation

Boundary remediation should begin with observed communication paths, not the old diagram. Identify internet paths, site-to-site connections, cloud peering, vendor access, RMM, VPN, management networks, wireless, application interfaces, and data transfers.

Corrections may involve rule cleanup, segmentation, dedicated administration paths, stronger remote authentication, protocol changes, encryption, removal of unused tunnels, or redesigned cloud connectivity. Validate from both permitted and prohibited paths and update diagrams only after the tested architecture is understood.

For network boundary and remote access remediation, Harbor Point also identifies documentation and evidence consequences. Any change that affects scope, responsibility, configuration, operating procedure, or provider dependency triggers updates to the relevant SSP sections, diagrams, inventories, and evidence index. This

keeps remediation from creating a technically improved but inaccurately documented environment.

8.20 Vulnerability and Patch Remediation

Vulnerability remediation must connect scanning, prioritization, change control, patch or configuration correction, exceptions, and rescanning. The objective is not to reduce the report count; it is to ensure the affected systems are corrected or otherwise handled through an approved process.

Work packages should address scan coverage, credentialed failures, unsupported systems, application vulnerabilities, reboot dependencies, emergency patching, and validation. Repeated overdue findings may reveal maintenance-window or ownership problems that require management action.

For vulnerability and patch remediation, Harbor Point also identifies documentation and evidence consequences. Any change that affects scope, responsibility, configuration, operating procedure, or provider dependency triggers updates to the relevant SSP sections, diagrams, inventories, and evidence index. This keeps remediation from creating a technically improved but inaccurately documented environment.

8.21 Incident Response and Escalation Remediation

Incident findings frequently involve unclear authority rather than missing tools. Map detection to triage, customer notification, containment authorization, reporting, preservation, recovery, and lessons learned. Then reconcile the customer plan, MSP procedure, SOC routing, contacts, and contract language.

Validate with exercises that include after-hours events, unavailable primary contacts, ambiguous alerts, provider handoffs, and evidence preservation. A successful tabletop should produce action items and updated records, not just a completion certificate.

For incident response and escalation remediation, Harbor Point also identifies documentation and evidence consequences. Any change that affects scope, responsibility, configuration, operating procedure, or provider dependency triggers updates to the relevant SSP sections, diagrams, inventories, and evidence index. This keeps remediation from creating a technically improved but inaccurately documented environment.

8.22 Backup, Recovery, and Continuity Remediation

Backup remediation should distinguish job success from recoverability. Identify which systems and information must be protected, where copies reside, who can administer them, how failures are handled, what restoration objectives matter, and how recovered information is validated.

Corrections can include coverage reconciliation, immutable or separated protections where appropriate, stronger administrator controls, failure escalation, documented restore procedures, and recurring restore tests. Business owners should validate whether recovered information is usable, not only whether the software reports success.

For backup, recovery, and continuity remediation, Harbor Point also identifies documentation and evidence consequences. Any change that affects scope, responsibility, configuration, operating procedure, or provider dependency triggers updates to the relevant SSP sections, diagrams, inventories, and evidence index. This keeps remediation from creating a technically improved but inaccurately documented environment.

8.23 Treat Documentation Gaps as Remediation Work, but Not as Substitute Work

Documentation gaps need owners and deadlines because contradictory records can undermine operations and assessment preparation. The correction, however, depends on the underlying condition. If the environment is correct and the SSP is stale, update the SSP. If the SSP describes the intended secure design but the system is configured differently, fix the system or formally redesign the intended state before rewriting the document.

Harbor Point links documentation tasks to the technical work package that establishes the authoritative state. The SSP owner does not update firewall descriptions while the network team is still deciding the new segmentation model. The responsibility matrix does not move an incident duty to NorthStar until the service agreement and operating process support that assignment.

This sequencing reduces churn and prevents paperwork from being used to make a gap appear closed. Documentation should follow verified reality and approved responsibility.

8.24 Remediate Evidence Gaps by Fixing the Evidence Process

When the control appears to operate but evidence is weak, the remediation should improve how evidence is generated, attributed, retained, protected, reviewed, and retrieved. Creating one screenshot for the readiness team may close the immediate presentation problem while leaving the evidence process fragile.

Harbor Point defines recurring evidence sources for high-value controls. Identity reviews produce approved exports. Vulnerability work produces scan, ticket, and rescan records. Backup testing produces restore results and business validation. Incident exercises produce scenario, participant, decision, and action records. Logging produces source-health and review evidence.

The evidence design should minimize manual reconstruction. Automated reports can help, but the team must still know what the report proves, who owns it, and how exceptions are handled. Evidence quality is a process requirement, not a folder-building exercise.

8.25 Remediate Provider Dependencies Through Facts, Contracts, or Architecture

A provider dependency can be resolved in several ways. The provider may supply the missing assurance or configuration evidence. The customer may change the service tier or enable a required feature. The MSP contract may be amended to include a responsibility that was assumed but not purchased. The organization may redesign the architecture to reduce or remove reliance on the provider.

The roadmap should record which path is being pursued and the decision deadline. Open-ended requests to vendors are dangerous because the rest of the program can stall while everyone assumes the provider will eventually answer. Management should know when to escalate, choose an alternative, or redesign.

Provider remediation should also consider transition risk. Replacing a service can create new identities, migrations, downtime, evidence gaps, and offboarding obligations. The roadmap should include continuity and verified termination of the old provider relationship.

8.26 Align Service Agreements with the Remediated Operating Model

If remediation changes what the MSP or security provider must do, the service agreement must support that work. Technical teams should not quietly absorb

recurring tasks that were never scoped, staffed, or priced. That creates an unsustainable control that may fail later when personnel or priorities change.

Harbor Point reviews agreements when remediation adds after-hours response, recurring access reviews, evidence retention, vulnerability validation, backup restore testing, new reporting, or customer-specific configuration management. The agreement should identify outcomes, responsibilities, service windows, exclusions, dependencies, and escalation routes.

Contract alignment is not merely commercial housekeeping. It helps demonstrate that the people and services relied upon by the SSP and responsibility matrix are actually authorized and resourced to perform the work.

8.27 Use Scope Reduction Carefully and Transparently

Reducing scope can be a legitimate architectural strategy when the organization can isolate CUI and security dependencies effectively. It should not be used as a paperwork technique to exclude systems that remain connected, administratively capable, or involved in security protection under the applicable scoping rules.

A roadmap may include moving CUI to an enclave, eliminating local downloads, separating administrative systems, restricting collaboration, or changing remote-work patterns. These projects can reduce long-term complexity but require careful data-flow, identity, network, and provider analysis.

Before declaring scope reduction successful, repeat the scoping process. Verify logical and physical separation, administrative paths, security protection data, provider relationships, and ordinary user behavior. Update the SSP and diagrams after the new architecture is tested.

8.28 Plan Training and Operational Adoption as Part of the Fix

A technically correct control can fail when users and technicians do not understand the new workflow. Remediation packages should therefore include role-specific communication and training when behavior changes. The training should explain what changed, why it changed, what exceptions are permitted, and how to request help.

For NorthStar technicians, new customer-specific administrative procedures may require changes to escalation, ticket fields, credential use, session documentation, or

approval. For Harbor Point users, the changes may involve authentication, approved storage, remote work, printing, or incident reporting.

Adoption should be validated through observation and records. If technicians continue using the old remote-support path after the policy changes, the remediation is not complete.

8.29 Reconcile Every Material Change with the Security Story

The security story consists of the scope, architecture, SSP, responsibility matrix, procedures, inventories, service agreements, and evidence. Material remediation can affect several of these records at once. The roadmap should therefore include a documentation impact field for every significant work package.

Harbor Point uses a reconciliation checklist at closure. Did the architecture change? Did a provider responsibility change? Did a new tool enter scope? Did the evidence source change? Did a recurring review gain a new owner? Did the incident plan or contact list change? Each yes answer points to controlled documentation that must be updated.

This step prevents the organization from passing an internal technical re-test while carrying contradictory documentation into the next assessment cycle.

8.30 Maintain an Internal Corrective-Action Register Separate from Formal POA&M Status

Every known weakness deserves management visibility. Formal CMMC POA&M treatment is narrower and governed by specific rules. Harbor Point therefore maintains an internal corrective-action register that includes all remediation items. A separate field indicates whether an item is considered for formal POA&M treatment under the applicable current requirements.

This prevents two dangerous assumptions: that an item not eligible for formal POA&M can be ignored, or that placing an item on a plan makes the requirement effectively met. Internal work tracking is about security and execution. Formal POA&M treatment is about the conditions allowed by the governing assessment process.

The compliance lead should verify current eligibility rules and time limits before making any external representation. The roadmap can carry the item regardless of its formal status.

8.31 Define Closure Criteria Before Implementation Begins

Closure criteria should be written before the work starts whenever practical. This prevents the implementer from deciding after the fact that whatever was deployed is good enough. The criteria should describe the expected result, coverage, negative conditions, evidence, and documentation updates.

For the EDR coverage finding, closure is not install agents on two laptops. Closure is that all current in-scope endpoints are reconciled against the approved inventory, required protection is active and healthy, unsupported exceptions are addressed, rebuild enrollment is corrected, and ongoing reconciliation is operating.

Clear criteria also make re-testing efficient. The reviewer knows what to examine and test, and the work owner knows what evidence to preserve during implementation.

8.32 Integrate Remediation with Change Management

Security projects should not bypass normal change controls simply because they are compliance-driven. Remediation can disrupt production, create new vulnerabilities, or invalidate evidence if changes are rushed. The roadmap should identify change category, approval, testing, maintenance window, rollback, and post-change validation.

Emergency corrections may use expedited processes, but the organization should preserve the reason for urgency and complete retrospective review. A critical access exposure may justify immediate disabling of a route; the durable configuration should still be designed and documented through controlled change.

Change records are also useful evidence because they connect the approved design to actual implementation. They should be specific enough to show what changed without becoming the only source of truth for the final configuration.

8.33 Validate Remediation Independently Enough to Challenge Assumptions

The person who implements a correction can demonstrate it, but closure benefits from a reviewer who can challenge the result. Small organizations may not have a completely independent audit team. They can still separate implementation from validation by using another qualified person, a peer review, or a structured test against predefined criteria.

Validation should reproduce the relevant condition. If the issue involved unauthorized access, test that the unauthorized path is denied. If the issue involved missing logs, verify that the expected event is generated, collected, retained, and reviewed. If the issue involved a failed offboarding process, trace a new termination event through all relevant identities.

Where validation cannot fully reproduce production conditions, record the limitation. Transparency is better than a stronger conclusion than the evidence supports.

8.34 Capture Closure Evidence During the Change, Not Weeks Later

Evidence is easiest to capture when the work happens. Waiting until a readiness deadline often forces engineers to reconstruct old configurations, find expired logs, or create screenshots that do not show the actual transition. Each work package should identify closure artifacts in advance.

NorthStar attaches approved design records, configuration exports, before-and-after evidence where useful, test results, exception decisions, and final review to the remediation record. Sensitive artifacts are stored in controlled repositories with customer attribution and access restrictions.

The evidence package should show enough context to understand the result. A screenshot of an enabled toggle may not establish coverage, scope, or enforcement. The team should preserve the authoritative configuration or report whenever practical.

8.35 Do Not Close the Finding Until the Process Can Survive Tomorrow

A remediation can work once and still be unsustainable. The roadmap should ask how the correction will survive new hires, rebuilds, new assets, provider turnover, software updates, emergency changes, and architecture growth. Sustainment is part of closure for controls that depend on recurring operation.

Harbor Point therefore adds monitoring and ownership to the final state. Identity groups have recurring review. Endpoint coverage is reconciled. Log-source health is monitored. Vulnerability exceptions expire. Provider evidence has a refresh trigger. Incident contacts are reviewed. SSP changes are tied to material change management.

This is the difference between assessment preparation and security operations. The organization should be able to maintain the state without recreating the remediation project every year.

8.36 Budget the Full Cost of Remediation

Remediation cost includes more than software licenses. It includes engineering design, implementation labor, customer coordination, maintenance windows, training, provider services, contract changes, migration, testing, evidence management, and ongoing operations. A cheaper tool can be more expensive if it requires extensive manual work or specialized support.

Harbor Point creates a total-cost view for each major program. Identity modernization includes licensing, integration, technician time, application testing, user support, and recurring access review. Logging improvements include ingestion, retention, storage, analyst effort, health monitoring, and evidence retrieval. Scope-reduction architecture includes migration and user workflow redesign.

Budget transparency helps management choose deliberately. If the organization cannot fund the required operating model, that is a business decision that needs escalation—not a reason to let the roadmap quietly assume free recurring labor.

8.37 Plan Capacity, Not Just Calendar Dates

A roadmap can contain realistic tasks and still fail because the same two engineers are assigned to every project. Capacity planning should consider named skills, not only headcount. Identity, firewall, cloud, application, evidence, contract, and incident work may require different expertise.

NorthStar maps remediation demand to available engineering hours and change windows. Harbor Point maps decisions and testing to business owners. Provider lead times are added explicitly. When capacity is insufficient, management chooses to add resources, reduce scope, change sequence, or accept a longer timeline.

This prevents dates from being treated as commitments unsupported by resources. A credible roadmap explains why dates are achievable.

8.38 Use Metrics That Measure Risk Reduction and Closure Quality

Ticket counts reward activity. A remediation program should measure outcomes. Useful metrics include high-impact gaps remaining, objectives revalidated, assets

brought into coverage, privileged identities reduced, stale accounts eliminated, log-source coverage, vulnerability aging, evidence retrieval success, and repeat findings.

Harbor Point also measures closure quality. How many findings reopened after validation? How many corrections required emergency exceptions? How many work packages were delayed by provider or decision dependencies? Which findings recurred? These indicators help management improve the remediation process itself.

A green dashboard should never hide an unresolved critical exception. Metrics need narrative context and exception review.

8.39 Prepare the Executive Decision Package

Some remediation decisions belong at the executive level because they affect cost, business process, architecture, customer commitments, or risk. The remediation team should present those decisions in a form that allows management to understand the security consequence and available choices.

A useful decision package states the finding, affected business capability, current exposure, target outcome, options, cost and schedule ranges, dependencies, interim protections, and consequence of delay. It should identify what the team recommends technically without disguising business tradeoffs.

The decision record becomes part of governance evidence. It also protects engineers from being forced to carry undefined exceptions indefinitely because no one made the business choice.

8.40 Harbor Point Case Study: Build the First Remediation Wave

Harbor Point’s gap assessment identified four immediate concerns: former provider technicians retained limited remote-support capability, two rebuilt engineering laptops lacked active endpoint protection, incident escalation records contradicted one another, and one cloud logging service had incomplete retention evidence. The team does not place all four into the same technical queue because they require different owners and evidence.

The remote-support finding becomes an identity and privileged-access work package. NorthStar removes the stale memberships, reviews the complete technician population, and changes onboarding and offboarding so customer-specific groups are reconciled to employment and assignment. Closure requires an access export, approved population, negative access test, and new review procedure.

The endpoint finding becomes a coverage and deployment work package. NorthStar restores protection, fixes the rebuild image, adds inventory-to-console reconciliation, and validates every in-scope endpoint. The incident finding becomes a joint governance and operations work package with Harbor Point, NorthStar, and Beacon. The cloud item remains a provider dependency until the tenant-specific evidence is obtained and evaluated.

8.41 Harbor Point Case Study: Sequence Architecture and Process Changes

The next wave addresses larger structural issues uncovered during the family reviews. Harbor Point has too many administrative paths, inconsistent log-source onboarding, and vulnerability scanning that does not automatically incorporate new cloud assets. NorthStar proposes an architecture program rather than three unrelated fixes.

The team first defines the authoritative asset and identity sources. It then redesigns privileged administration around fewer approved paths, integrates new-asset onboarding with logging and vulnerability processes, and establishes health reconciliation. Application owners pilot the design before enforcement. Provider and licensing changes are approved early because they are schedule dependencies.

The roadmap shows which documentation waits on the architecture decision and which interim controls protect the environment. This prevents the SSP from being rewritten repeatedly while the design is still changing.

8.42 Harbor Point Case Study: Validate Closure and Sustainment

At the end of each remediation wave, Harbor Point conducts a validation review. Work-package owners present the original finding, target state, change records, evidence, test results, and documentation updates. Reviewers challenge coverage and exceptions. Items that pass move to closed; items that partially pass return to active or blocked with the remaining condition identified.

The endpoint package initially fails closure because one rarely used engineering laptop has been offline during the validation window. Rather than hiding the device, the team records it as an unresolved coverage condition, schedules controlled validation when it returns, and keeps the finding open for that asset. This is the kind of disciplined decision that prevents optimistic closure from weakening the program.

Once closure is complete, recurring monitoring becomes the sustainment mechanism. Coverage reconciliation, access reviews, provider evidence refresh, incident exercises, vulnerability validation, and change-driven SSP updates move into ordinary operations.

8.43 Run the Remediation Roadmap Workshop

A roadmap workshop should convert technical findings into approved work. Invite finding owners, technical leads, business owners, provider representatives where needed, the SSP owner, procurement or contracts personnel for service changes, and management capable of resolving priorities and resources.

Begin with the highest-impact clusters rather than reading every finding row. Define target outcomes, containment, dependencies, ownership, decision points, validation, evidence, and documentation impact. Then place work into waves based on dependency and capacity. Record disagreements as explicit decisions or actions rather than forcing vague consensus.

The workshop should end with an executable roadmap, not a colorful heat map. Every active work package needs a next action. Every blocked item needs a named blocker. Every major decision needs an owner and date. Every planned closure needs a validation method.

- Confirm the current finding register and affected scope.
- Cluster related findings by root cause, platform, or dependency.
- Identify immediate containment for high-impact open conditions.
- Define target state and closure criteria for each work package.
- Map technical, provider, procurement, and management dependencies.
- Assign one outcome owner and required contributors.
- Place work into waves based on risk, dependency, and capacity.
- Approve validation, evidence, and documentation update requirements.
- Record executive decisions, funding needs, and unresolved blockers.
- Schedule roadmap review and re-testing checkpoints.

Detailed Remediation Field Guide

The following field guide translates common MSP/customer gap patterns into remediation design. It is intentionally operational. Each guide explains the condition, immediate containment, durable correction, validation, evidence, and sustainment. These examples are not mandatory CMMC solutions. They show how to structure corrective work so that the final state can be demonstrated and maintained.

Remediation Field Guide 1: Privileged access sprawl

Observed condition: Multiple administrator groups, local accounts, provider roles, and emergency paths exist without one authoritative population or consistent MFA.

Immediate containment: Remove unnecessary standing access and disable clearly unauthorized paths after appropriate approval. Increase monitoring on emergency paths while redesign is underway.

Durable correction: Create an authoritative privileged identity inventory, reduce administration to approved paths, enforce required authentication, assign account owners, establish time-bounded emergency procedures, and schedule recurring access review.

Validation approach: Compare approved population to every privileged path. Test authorized and unauthorized access. Review authentication and session logs.

Closure evidence: Approved population, group/role exports, policy configuration, test results, access-review approval, exception records.

Sustainment: Trigger review after technician changes, customer role changes, new management platforms, and material architecture changes.

MSP implementation note: The work package should identify which actions belong to the customer, the MSP, the security provider, or another external service. If recurring work is added, confirm that the service agreement and staffing model support it. If the correction changes scope or architecture, repeat the appropriate scoping analysis before closure.

Remediation Field Guide 2: Unmanaged endpoint or agent coverage

Observed condition: The asset inventory contains systems that do not appear healthy in EDR, patching, logging, vulnerability, or configuration consoles.

Immediate containment: Identify missing high-risk assets and restore protection where safe. Restrict or isolate assets that cannot immediately be brought under management.

Durable correction: Fix enrollment and rebuild workflows, reconcile authoritative inventory to each required management platform, define health thresholds, and assign exception handling.

Validation approach: Reconcile full populations; inspect representative assets; simulate a failed or missing agent; verify alert and restoration workflow.

Closure evidence: Inventory exports, console coverage, health reports, enrollment configuration, exception approvals, test results.

Sustainment: Automate or schedule reconciliation and review unresolved exceptions at a defined cadence.

Remediation Field Guide 3: Log-source gaps

Observed condition: Required systems do not send expected events, retention is unclear, or failed collectors are not detected.

Immediate containment: Restore missing critical sources and increase local review where centralized telemetry is temporarily unavailable.

Durable correction: Build a source-to-event matrix, configure required logging, centralize or protect records, monitor collector health, define retention, and connect review to incident escalation.

Validation approach: Generate safe events from representative sources, confirm receipt and attribution, test source failure detection, and retrieve historical records.

Closure evidence: Source inventory, configuration, event samples, health alerts, retention settings, review tickets.

Sustainment: Onboard logging through asset/change workflows and review health exceptions continuously.

Remediation Field Guide 4: Stale or contradictory SSP

Observed condition: The SSP, diagrams, responsibility matrix, and real implementation disagree.

Immediate containment: Do not rewrite documents until the team determines the authoritative current state and whether the technology or documentation is wrong.

Durable correction: Correct the implementation if needed, then update controlled records together so scope, responsibility, architecture, and evidence sources agree.

Validation approach: Walk representative workflows against the revised records and technical configuration.

Closure evidence: Approved revisions, change history, diagrams, matrix updates, technical validation.

Sustainment: Tie SSP review to material change management and periodic governance.

Remediation Field Guide 5: Vulnerability findings that never truly close

Observed condition: Tickets close when patches are deployed even though rescans still show exposure.

Immediate containment: Reopen affected high-risk items, restrict exposure where necessary, and verify whether patches or configuration changes actually took effect.

Durable correction: Require validation criteria and rescans, track failed deployments and reboot dependencies, govern exceptions, and reconcile scan coverage to assets.

Validation approach: Trace selected findings from discovery through verified absence or approved disposition.

Closure evidence: Scan results, remediation tickets, patch/change records, rescans, exception approvals.

Sustainment: Measure aging, reopen rates, failed scans, and repeat vulnerabilities.

Remediation Field Guide 6: Provider evidence unavailable

Observed condition: The customer depends on a service but cannot retrieve the configuration, assurance, or operational evidence needed to support the implementation.

Immediate containment: Document the dependency and avoid overstating the conclusion. Identify interim customer-side evidence that is valid without pretending it proves provider behavior.

Durable correction: Obtain service-specific provider evidence, change service tier or contract, enable reporting, or redesign the architecture to reduce the dependency.

Validation approach: Test the new retrieval path and confirm the evidence applies to the exact offering, tenant, and period.

Closure evidence: Provider CRM or service description, assurance artifacts, tenant reports, contract terms, retrieval test.

Sustainment: Assign refresh triggers for provider documentation and material service changes.

Remediation Field Guide 7: Incident escalation ambiguity

Observed condition: Customer, MSP, and SOC documents name different contacts or containment authority.

Immediate containment: Publish an interim verified contact route and escalation rule while the formal process is reconciled.

Durable correction: Define decision authority, technical authority, notification sequence, reporting responsibility, evidence preservation, after-hours coverage, and backup contacts across all parties.

Validation approach: Run a tabletop that includes ambiguous alerts, unavailable contacts, and containment decisions.

Closure evidence: Updated plans, contact lists, service terms, exercise records, action closure.

Sustainment: Review after personnel/provider changes and at recurring exercise intervals.

Remediation Field Guide 8: Backup success without recoverability proof

Observed condition: Backup jobs report success but restorations are rarely tested or business owners do not validate recovered information.

Immediate containment: Confirm protection of the highest-value systems and perform targeted restores where risk is greatest.

Durable correction: Reconcile backup coverage to assets/data, strengthen admin access, define recovery procedures and objectives, schedule representative restore testing, and record business validation.

Validation approach: Perform restores to approved locations, verify integrity/usability, test failure escalation, and review provider dependencies.

Closure evidence: Coverage reports, job failures, restore logs, business validation, admin access review.

Sustainment: Recurring restore tests, coverage reconciliation, and review after major system changes.

Remediation Field Guide 9: Training population mismatch

Observed condition: People with system or provider access are absent from required awareness or role training reports.

Immediate containment: Identify untrained privileged personnel and apply the approved interim access/training response.

Durable correction: Define authoritative training populations from HR, contractor, and privileged-access sources; automate assignment where practical; add customer-specific instruction for provider staff.

Validation approach: Reconcile active access to training completion and sample recent hires/role changes.

Closure evidence: Training roster, access population, completion reports, escalation records.

Sustainment: Recurring reconciliation and trigger-based training after role changes.

Remediation Field Guide 10: Remote work handling weakness

Observed condition: Policies exist but users store, print, or access CUI through uncontrolled home or travel workflows.

Immediate containment: Restrict clearly unapproved pathways and remind affected users of approved methods.

Durable correction: Redesign remote access, storage, printing, device, and physical-handling controls; provide practical user guidance; reduce local data movement where possible.

Validation approach: Observe approved remote workflow, verify device controls and access restrictions, and interview users.

Closure evidence: Remote-work policy, device configuration, access logs, acknowledgements, exception records.

Sustainment: Review after technology changes, travel patterns, or new remote-work models.

Model Remediation Roadmap Record

Field	Example for Harbor Point
Finding ID	HP-AC-004
Condition	Former provider technicians remain in a shared support group capable of initiating limited sessions
Target state	Only currently authorized NorthStar technicians can initiate Harbor Point remote support using the approved authenticated path
Containment	Remove known stale memberships and review recent session activity
Root cause	Provider offboarding not reconciled to customer-specific shared support groups
Owner	NorthStar Service Delivery Manager
Contributors	Harbor Point security coordinator; NorthStar IAM lead; service desk
Dependencies	Current technician roster; customer support group inventory; approved emergency access model
Implementation	Group cleanup, automated offboarding linkage, access review workflow, session monitoring
Validation	Compare approved roster to roles; negative test removed account; review session attribution
Evidence	Approved roster, exports, ticket/change record, test result, review approval
Documentation	Responsibility matrix; remote-support procedure; SSP administrative access description
Sustainment	Monthly provider privileged-access reconciliation and trigger after technician termination/transfer
Closure authority	Harbor Point security coordinator after independent validation

Control-Family Remediation Playbooks

The Level 2 families are interconnected, but remediation teams still need a practical way to organize work. The playbooks below do not prescribe a single technical solution. They provide a disciplined structure for moving from a family-level finding to a corrected and supportable operating state. Each playbook should be tailored to the actual scope, requirement objectives, provider model, and customer architecture.

Playbook 1: Access Control (AC)

Access decisions are not only technical settings. They begin with business authorization and end with verified enforcement across applications, endpoints,

networks, remote support, local administration, cloud roles, and provider access. Remediation therefore has to close both the decision gap and the enforcement gap.

A useful remediation effort begins by determining whether the observed issue is isolated or systemic. The team should review the original evidence, identify affected populations, and test whether the same failure pattern appears in related systems or workflows. The work package should address the complete affected population rather than the first example that exposed the gap.

Common findings that can drive remediation

- Stale user or technician access
- Excessive inherited group permissions
- Remote administration paths outside the normal MFA design
- Temporary access that never expires
- Application roles that are not included in enterprise access reviews
- Local administrator credentials that are difficult to attribute

Recommended remediation sequence

1. Establish the authoritative user, provider, service-account, and privileged-access populations.

2. Map every meaningful path by which a user or provider can reach the assessed environment.

3. Remove clearly unnecessary standing access after appropriate review and preserve the change evidence.

4. Define role models and approval criteria so technicians are not forced to copy existing users as permission templates.

5. Enforce required authentication and session controls consistently across the approved paths.

6. Add periodic review that covers customer identities, provider identities, local accounts, application roles, and emergency access.

7. Link onboarding, transfer, and offboarding events to the access systems that must change.

The sequence should be adjusted when containment is required. High-impact unauthorized access, missing protection, or failed monitoring may justify immediate restrictions before the durable design is complete. The interim action should be documented, reviewed, and retired when the final architecture is validated.

Validation and closure evidence

- Approved access population and owner
- Role/group export before and after cleanup
- Remote-access configuration
- MFA or authentication enforcement
- Representative access request and implementation record
- Periodic review approval
- Negative test for removed or unauthorized access

Validation should challenge both positive and negative conditions. Demonstrating that an authorized user can work is not enough when the finding concerned unauthorized access. Demonstrating that a log event exists is not enough when the finding concerned retention or failed-source detection. Closure tests should reproduce the security outcome that the original finding questioned.

NorthStar should not treat its RMM console as separate from Harbor Point access governance simply because the console is provider-owned. If the console can administer in-scope systems, provider technician authorization, authentication, role assignment, and session evidence become part of the customer security story.

Sustainment should be designed before closure. Identify the recurring review, health check, ownership, or change trigger that keeps the correction operating. If the work introduces a new recurring duty for the MSP, confirm that the service agreement, staffing model, access, tooling, and evidence process support the duty. If the work changes architecture or information flow, repeat the appropriate scope analysis before final closure.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work

	as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 2: Awareness and Training (AT)

Training remediation is successful when the people who can affect the environment understand the behaviors and decisions expected of them. A training platform can record completion, but the roadmap must ensure that the right population receives the right instruction and that specialized roles receive more than general awareness content.

Common findings that can drive remediation

- Contractors or provider technicians missing from the required population
- Privileged administrators receiving only generic awareness training
- Customer-specific handling rules not taught to MSP staff
- Overdue training with no escalation
- New access granted before required instruction
- Training records that cannot be tied to current roles

Recommended remediation sequence

1. Define authoritative training populations from HR, contractor, and privileged-access data.
2. Map role-specific instruction to technical and business responsibilities.
3. Create customer-specific instructions for provider personnel where the service requires unique handling or escalation.
4. Automate assignment at onboarding and role change where practical.
5. Define escalation and access consequences for overdue training.
6. Reconcile the training population to active access on a recurring basis.
7. Refresh instruction after material process, technology, or incident changes.

Validation and closure evidence

- Training roster
- Role-to-training matrix
- Completion records
- Overdue escalation record
- Customer-specific instruction acknowledgement
- Sample of recent hires or role changes
- Periodic population reconciliation

An MSP may have an excellent corporate awareness program and still need remediation if the technicians supporting Harbor Point do not understand customer-specific CUI handling, remote-support limitations, incident escalation, or evidence procedures.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 3: Audit and Accountability (AU)

Audit remediation should make activity reconstructable and reviewable. The program needs to know which systems should generate which events, where those events go, how long they remain available, who reviews them, how privileged activity is identified, and what happens when telemetry stops.

Common findings that can drive remediation

- Important assets missing from centralized logging
- Inconsistent event selection

- Retention shorter than the approved design
- Collector or agent failures that go unnoticed
- Privileged provider activity not attributable to individuals
- Review records that show alerts but not investigation outcomes

Recommended remediation sequence

1. Create a source-to-event matrix tied to the in-scope asset inventory.
2. Enable required event categories on representative system types and standardize deployment.
3. Centralize or otherwise protect audit information consistent with the architecture.
4. Configure source-health monitoring and escalation for collection failures.
5. Define retention based on the approved security and contractual design.
6. Map privileged human identities to logged activity, including provider sessions.
7. Create review workflows that record disposition and incident escalation when appropriate.

Validation and closure evidence

- Source inventory
- Audit configuration
- Representative event samples
- Health-monitoring alerts
- Retention settings
- Privileged activity report
- Review ticket and disposition
- Evidence of response to a failed source

Beacon and NorthStar may operate different parts of the logging chain. The remediation package should show where NorthStar enables or forwards logs, where Beacon receives and analyzes them, who owns source-health failures, and what Harbor Point receives as customer evidence.

Closure checkpoint	Question

Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 4: Configuration Management (CM)

Configuration remediation should create a controlled relationship between approved baselines and deployed systems. The organization should be able to explain the secure baseline, who can change it, how changes are authorized, how emergency work is handled, and how drift or unauthorized software is identified.

Common findings that can drive remediation

- Baselines exist only as documents and are not enforced
- Global MSP scripts changed without customer impact review
- Emergency changes never receive retrospective approval
- Configuration drift is discovered only during assessment
- Software inventories contain unknown or unapproved applications
- Exceptions lack owner or expiration

Recommended remediation sequence

1. Select authoritative baseline sources for each technology class.

2. Translate baseline expectations into configuration mechanisms, automation, or controlled procedures.

3. Restrict who can modify templates and scripts and require versioned change control.

4. Create exception records with reason, affected assets, approver, expiration, and validation.

5. Implement drift or compliance reporting where practical and define how deviations are handled.

6. Review emergency changes after the event and incorporate justified permanent changes into the baseline.

7. Reconcile software and configuration inventories to actual deployed systems.

Validation and closure evidence

- Baseline document and technical policy
- Change approvals
- Script or policy version history
- Drift report
- Exception register
- Emergency-change review
- Representative system comparison

NorthStar should distinguish provider-global automation from Harbor Point-specific configuration. Remediation must prevent a generic MSP standard from silently overwriting a customer control or from creating undocumented exceptions.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 5: Identification and Authentication (IA)

Identification and Authentication remediation should eliminate unmanaged identity paths and strengthen the lifecycle of credentials and authenticators. The team needs

one coherent model for workforce, privileged, service, local, device, application, API, and emergency identities.

Common findings that can drive remediation

- Local or break-glass accounts outside normal MFA
- Shared service accounts used interactively
- Legacy applications bypassing the primary identity provider
- Provider technician identities not clearly mapped to human users
- Stale API keys or automation credentials
- Authenticator reset processes with weak verification

Recommended remediation sequence

1. Inventory all identity classes and authentication paths.
2. Assign owners to non-human and emergency identities.
3. Reduce or isolate legacy paths that cannot meet the intended authentication design.
4. Enforce required MFA or other authentication controls across approved access paths.
5. Implement credential rotation and revocation for service and automation identities.
6. Strengthen reset and recovery procedures with documented identity verification.
7. Monitor authentication exceptions and review them on a defined schedule.

Validation and closure evidence

- Identity inventory
- MFA and conditional-access configuration
- Service-account ownership
- Authentication logs
- Credential rotation record
- Emergency account procedure
- Negative authentication test after revocation

Provider identities deserve the same level of rigor as customer identities when they can administer the assessed environment. A provider should be able to demonstrate

unique technician identity, strong authentication, role assignment, and revocation after employment or assignment change.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 6: Incident Response (IR)

Incident-response remediation should create a single executable chain from detection through decision, containment, reporting, preservation, recovery, and lessons learned. Most difficult findings occur at organizational boundaries where the SOC, MSP, customer management, and contract personnel assume that another party owns the next decision.

Common findings that can drive remediation

- Different documents name different escalation routes
- No one knows who may isolate a production system
- After-hours contacts are outdated
- Government or prime-contractor reporting decisions are not integrated into the technical process
- Evidence-preservation steps are unclear
- Exercises exclude external providers

Recommended remediation sequence

1. Map the complete incident workflow across all parties.
2. Assign decision authority separately from technical execution.
3. Reconcile SOC, MSP, customer, legal, and contract contacts.

4. Define after-hours and unavailable-contact escalation.

5. Document preservation and reporting decision points.

6. Update service agreements where recurring response work changes.

7. Run tabletop exercises that include ambiguous alerts, containment choices, provider handoffs, and reporting decisions.

8. Track lessons learned to closure and update procedures.

Validation and closure evidence

- Incident plan
- Provider escalation procedure
- Current contact matrix
- Tabletop scenario and results
- Containment decision record
- Preservation evidence
- After-action corrective actions

NorthStar should know when it is authorized to act immediately and when Harbor Point must decide. Beacon should know who receives critical alerts and what information the customer needs to make that decision. Remediation should remove delay caused by uncertainty.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 7: Maintenance (MA)

Maintenance remediation should govern the people, tools, sessions, and devices involved in authorized support. Routine remote administration can hide maintenance risk when provider technicians have broad standing access or vendor support channels remain enabled indefinitely.

Common findings that can drive remediation

- Persistent vendor support accounts
- Remote maintenance not attributable to individual technicians
- Temporary tools or accounts left behind
- Device repair or return workflows that do not address protected information
- Customer authorization not visible in maintenance records
- Uncontrolled out-of-band support paths

Recommended remediation sequence

1. Inventory maintenance paths and vendor support arrangements.
2. Require individual technician identity and approved authentication.
3. Time-limit temporary accounts and vendor access where practical.
4. Define customer authorization for sensitive maintenance actions.
5. Control diagnostic tools and removal after use.
6. Document device handling, sanitization, or replacement procedures.
7. Review remote session evidence and provider access periodically.

Validation and closure evidence

- Maintenance ticket
- Remote session log
- Temporary account lifecycle
- Vendor authorization
- Tool inventory
- Device handling record
- Post-maintenance validation

Because MSP RMM tools provide persistent capability, remediation should show how NorthStar limits maintenance privilege, detects misuse, separates customers, and removes access when a technician no longer needs Harbor Point support rights.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 8: Media Protection (MP)

Media remediation should follow information into all forms in which it can be stored or transported. USB restrictions alone are not enough. Printed drawings, exported spreadsheets, support attachments, backup media, replacement drives, mobile devices, and diagnostic packages may all create handling obligations.

Common findings that can drive remediation

- Uncontrolled removable media
- Support screenshots or exports stored in ordinary tickets
- Failed drives returned without approved sanitization
- Printed CUI stored in shared areas
- Backup media ownership unclear
- Users create local copies outside the approved workflow

Recommended remediation sequence

1. Map media and export pathways from real work.

2. Restrict or approve removable-media use and enforce technical controls where practical.

3. Define approved print, storage, transport, and destruction practices.

4. Move sensitive support artifacts into controlled workflows.
5. Implement sanitization and destruction evidence for retired or returned storage.
6. Train users and technicians on customer-specific media handling.
7. Review exceptions and exports periodically.

Validation and closure evidence

- Device-control configuration
- Media inventory
- Approved exception
- Encryption status
- Destruction or sanitization record
- Support artifact handling record
- Remote/print workflow observation

NorthStar should consider the artifacts its own technicians create. A screenshot captured during troubleshooting can create the same information-handling problem as the original customer file if it contains CUI or security protection data.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 9: Personnel Security (PS)

Personnel remediation should ensure that hiring, screening, transfer, termination, and provider staffing events reliably trigger security action. The strongest technical access controls can still fail if personnel events do not reach the systems that must change.

Common findings that can drive remediation

- Terminations remove the primary account but miss application or provider access
- Role transfers accumulate permissions
- Provider technician changes rely on informal memory
- Physical and logical access changes occur at different times
- Screening or personnel assurance is unclear for provider staff
- Urgent terminations have no expedited process

Recommended remediation sequence

1. Map personnel events to every logical and physical access system.
2. Integrate HR or provider staffing notifications with service desk and identity workflows.
3. Create customer-specific provider access removal checks.
4. Define urgent termination procedures and verification.
5. Review transferred users for accumulated privileges.
6. Establish provider assurance and notification expectations.
7. Sample personnel events periodically to verify end-to-end completion.

Validation and closure evidence

- HR or staffing notice
- Provisioning/deprovisioning tickets
- Identity and group exports
- Badge or physical access changes
- Provider roster
- Termination validation

NorthStar offboarding should not stop at disabling the technician in its corporate identity provider. Harbor Point-specific groups, vault permissions, local credentials, and application access must also be considered and verified.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected

	population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 10: Physical Protection (PE)

Physical remediation should protect the places where systems, media, and information actually exist. Cloud hosting does not eliminate physical obligations for laptops, networking equipment, server rooms, paper, alternate work sites, and customer facilities.

Common findings that can drive remediation

- Shared keys with no attribution
- Visitor records that are incomplete or never reviewed
- Server rooms accessible to general office traffic
- Remote-work storage expectations that users do not understand
- Former personnel retain badges or keys
- Provider physical assurance cited for customer-held assets

Recommended remediation sequence

1. Identify every relevant physical location and asset class.
2. Establish authorized access populations and individual access devices where practical.
3. Strengthen visitor authorization, escort, and recordkeeping.
4. Control server/network spaces and sensitive storage areas.
5. Reconcile terminations to physical access.
6. Define practical alternate-work-site rules for devices and paper.

7. Document provider facility reliance only where it applies to the selected service.

Validation and closure evidence

- Authorized access list
- Badge/key record
- Visitor log
- Facility observation
- Remote-work acknowledgement
- Termination sample
- Provider facility assurance

The MSP may host equipment or manage customer networking remotely, but Harbor Point still owns physical conditions at its offices and employee work sites unless a different responsibility is clearly documented and valid.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 11: Risk Assessment (RA)

Risk Assessment remediation should make both organizational risk review and vulnerability management operational. Scanner deployment alone is insufficient if asset coverage, authenticated scanning, application scope, exception decisions, and validation are weak.

Common findings that can drive remediation

- Critical assets absent from scanner targets

- Credentialed scans silently fail
- Application vulnerabilities are excluded
- Exceptions never expire
- Findings close before rescans
- Risk assessments are generic and disconnected from architecture changes

Recommended remediation sequence

1. Reconcile vulnerability targets to the authoritative asset inventory.
2. Monitor scan authentication and coverage failures.
3. Include applications and cloud resources according to the approved scope.
4. Define remediation and risk exception ownership.
5. Require rescans or equivalent verification before closure.
6. Review aging and repeated vulnerabilities for root cause.
7. Refresh organizational risk assessment after material architecture, provider, threat, or business changes.

Validation and closure evidence

- Coverage reconciliation
- Scanner configuration
- Authenticated scan result
- Remediation ticket
- Exception approval
- Rescan
- Risk assessment revision

A managed scanning service should not allow Harbor Point to lose visibility into remediation ownership. NorthStar may operate the scanner, but the customer and system owners still need a defined process for decisions, maintenance windows, exceptions, and closure.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected

	population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 12: Security Assessment (CA)

Security Assessment remediation should create a continuous cycle in which controls are evaluated, weaknesses are tracked, corrections are validated, and the SSP remains current. The program should not depend on one large readiness event every few years.

Common findings that can drive remediation

- Closed findings lack re-test evidence
- The SSP is updated only before assessment
- Continuous-monitoring reports are produced but not reviewed
- Corrective actions have dates but no validation plan
- Repeat findings indicate unresolved root cause
- Management does not review unresolved material gaps

Recommended remediation sequence

1. Define recurring internal assessment and monitoring activities.
2. Create a corrective-action register with stable finding IDs and closure evidence.
3. Require re-testing for material findings.
4. Tie SSP maintenance to material change and remediation closure.
5. Establish management review of overdue or high-impact items.
6. Analyze repeat findings for systemic causes.
7. Preserve assessment and remediation history in a controlled repository.

Validation and closure evidence

- Assessment plan
- Finding register
- Re-test evidence
- SSP revision history
- Monitoring reports
- Management review record
- Repeat-finding analysis

NorthStar can support monitoring and evidence production, but Harbor Point should retain visibility into the overall control-assessment program and ensure provider reports are actually reviewed and acted upon.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 13: System and Communications Protection (SC)

System and Communications Protection remediation should align architecture diagrams, boundary controls, remote access, encryption, key management, sessions, and cloud connectivity with the intended security model. This family often requires the most careful change planning because boundary changes can disrupt business applications.

Common findings that can drive remediation

- Firewall rules broader than documented
- Cloud peering or vendor tunnels absent from diagrams

- Remote-support channels bypass standard network paths
- Certificates or keys lack clear ownership
- Encryption is assumed but not verified
- Legacy protocols remain enabled for convenience

Recommended remediation sequence

1. Map observed network and communication paths.
2. Remove unused or unjustified rules and connections.
3. Segment sensitive systems and administration paths where the architecture requires it.
4. Standardize secure protocols and encryption settings.
5. Assign key and certificate ownership, renewal, and revocation.
6. Control collaborative-device and remote-session behavior.
7. Test allowed and denied paths and update diagrams after validation.

Validation and closure evidence

- Current network/data-flow diagram
- Firewall/security-group export
- Approved connection record
- Encryption configuration
- Certificate/key inventory
- Path test results
- Remote-support architecture

MSP administrative channels must appear in the architecture story. A provider-owned tunnel or RMM relay can be security-relevant even when ordinary users never see it.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?

Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Playbook 14: System and Information Integrity (SI)

System and Information Integrity remediation should establish a reliable lifecycle for flaw correction, malicious-code protection, advisories, monitoring, and unauthorized-use detection. Coverage and exception handling are central because security products protect only the systems actually enrolled and healthy.

Common findings that can drive remediation

- EDR agents unhealthy or missing
- Patch jobs report success without verifying final state
- Exclusions are broad or undocumented
- Unsupported systems sit outside normal remediation
- Advisories are received but not mapped to assets
- Repeated malware or integrity alerts are closed without root-cause action

Recommended remediation sequence

1. Reconcile asset inventory to endpoint protection and patching populations.
2. Define health monitoring and restore coverage when agents fail.
3. Govern exclusions with owner, reason, expiration, and review.
4. Improve patch validation, including reboot or service restart dependencies.
5. Create an advisory applicability process tied to asset/software inventory.
6. Establish treatment for unsupported systems, including isolation, upgrade, replacement, or approved alternative.
7. Analyze repeat integrity events for systemic weakness.

Validation and closure evidence

- Asset-to-agent reconciliation

- Patch deployment and validation
- EDR health report
- Exclusion approval
- Advisory applicability record
- Unsupported system treatment
- Repeat-event analysis

MSP dashboards can create false comfort when they emphasize percentages. The missing one percent may include the most important engineering server. Harbor Point should review the exception population behind the metric.

Closure checkpoint	Question
Coverage	Did the correction reach the full affected population?
Authority	Were required business and security decisions approved?
Operation	Does the technical or procedural mechanism work as designed?
Evidence	Can an authorized reviewer retrieve persuasive closure evidence?
Documentation	Do SSP, diagrams, procedures, and responsibility records match the final state?
Sustainment	Will the corrected state remain visible after personnel, asset, or provider changes?

Remediation Program Governance Toolkit

The technical playbooks solve control problems, but a large remediation program also needs management machinery. Without governance, high-priority tasks compete with customer operations, provider work stalls without escalation, and work closes before validation. The following tools make the roadmap executable and auditable.

Weekly remediation control meeting

Use a short operational meeting to review only items that require coordination, decision, or escalation. Do not read every row. Review high-impact open findings, blocked dependencies, upcoming change windows, validation failures, and new scope consequences. Every discussed item should end with a named next action and date.

Useful outputs include blocker escalation, dependency decisions, maintenance-window approval, provider follow-up, validation scheduling, and risk visibility.

NorthStar and Harbor Point should agree who maintains this governance record and how it is versioned. Governance artifacts can themselves become useful evidence of sustained management, but their primary purpose is to keep the remediation program from drifting away from the security outcomes it is supposed to achieve.

Executive steering review

Use a less frequent executive review for decisions that affect budget, architecture, business process, customer commitments, or risk. Provide concise decision packages rather than raw technical tickets.

Useful outputs include funding, architecture approval, scope strategy, provider replacement, staffing, schedule changes, and acceptance of operational disruption needed to reach the target state.

Dependency register

Track prerequisites outside the work package owner’s direct control. Include provider responses, procurement, contract amendments, licensing, application compatibility, maintenance windows, data migration, and management decisions.

A blocked status should identify the exact dependency and escalation path. This prevents vague waiting states and allows schedule impact analysis.

Validation calendar

Schedule re-testing separately from implementation. Reserve reviewer capacity and maintenance windows before the technical work completes so closure does not wait weeks for a test.

The calendar should include objective, environment, tester, expected evidence, prerequisites, and fallback if the system is unavailable.

Documentation impact register

For each major change, identify affected SSP sections, diagrams, inventories, procedures, provider descriptions, responsibility rows, contact lists, and evidence sources.

This avoids technically successful remediation that leaves assessment documentation contradictory.

Exception aging review

Temporary exceptions should have owner, reason, affected scope, interim protection, expiration, and review. Aging review forces management to choose extension, redesign, or closure.

Repeated extensions are a signal that the roadmap may need a larger architecture or resource decision.

Evidence readiness review

Select closed work packages and ask another person to retrieve the closure evidence without help from the implementer.

This reveals hidden dependencies on individual memory, portal access, provider contacts, or undocumented file locations.

Scope impact gate

Require a scoping review before implementing major tools, integrations, administrative paths, data migrations, cloud services, or enclave changes.

The gate asks whether new assets process, store, transmit, protect, administer, or connect to the assessed environment in ways that change the boundary or evidence obligations.

Worked Remediation Scenarios

The following scenarios show how a roadmap changes when the same technical weakness appears in different business and provider contexts. The objective is to practice reasoning about target state, containment, dependency, evidence, and sustainment rather than memorizing one preferred technology.

Scenario 1: MFA exists, but not on the RMM path

Harbor Point uses strong MFA for cloud identities, yet NorthStar technicians can reach endpoints through an RMM console authenticated only by the MSP corporate identity system. The team first determines whether the provider path satisfies the applicable authentication requirements and whether individual technicians are strongly authenticated. If not, containment may restrict the RMM population and increase session monitoring. Durable remediation may require stronger provider MFA, customer-specific role design, elimination of shared credentials, and confirmation that alternate local paths do not bypass the new model. Closure

evidence should include provider identity policy, authorized technician roster, role export, session attribution, and representative access tests.

Roadmap lesson: define the target state in observable terms, identify interim protection if needed, make dependencies explicit, and decide closure evidence before implementation. If the scenario changes scope, provider responsibility, or recurring service duties, update those records as part of the same work package rather than treating them as later paperwork.

Scenario 2: Vulnerability scanning shows 98 percent coverage

The dashboard looks strong until the missing assets are identified as a domain controller and an engineering application server. The roadmap should not celebrate the percentage. Immediate work restores coverage or applies approved interim restrictions. Root-cause analysis asks why inventory and scanning diverged. Durable remediation integrates new-asset onboarding, monitors failed authenticated scans, assigns exception ownership, and requires rescan validation. The metric changes from percentage alone to expected assets versus successfully assessed assets with named exceptions.

Scenario 3: The policy is correct but technicians use a shortcut

Harbor Point requires manager approval before privileged role assignment. Service desk staff have learned that urgent engineering requests are usually approved, so they sometimes add the role first and collect email approval later. Remediation should address workflow pressure, not only technician training. The team can redesign the request system so approval is fast, visible, and technically required before assignment. Emergency elevation should have a defined route with time limits and review. Validation samples urgent and normal requests and confirms that unauthorized pre-approval elevation is blocked or detected.

Scenario 4: Cloud provider evidence is delayed

Harbor Point depends on a SaaS platform for CUI-related workflow, but the selected service tier does not expose the audit retention report NorthStar expected. The roadmap records a provider evidence dependency rather than declaring the objective met. Procurement evaluates an upgraded service tier, alternate provider assurance, or migration. Interim evidence can include customer-side settings and event retrieval where valid, but the team clearly states the limitation. The decision package includes

cost, migration risk, schedule, and the consequence of continuing without provider evidence.

Scenario 5: Incident containment authority is unclear

Beacon identifies suspicious privileged activity at 2 a.m. The SOC contacts NorthStar, but the MSP contract says the customer authorizes containment while the customer incident plan says the SOC may isolate systems. The remediation package must reconcile authority, contacts, and contract language. An interim rule can identify who decides until the documents are corrected. The final validation is an after-hours tabletop with the primary Harbor Point contact unavailable. The test succeeds only if the backup route produces an authorized decision and the record shows what happened.

Scenario 6: EDR agents are reinstalled, but the rebuild problem remains

Two rebuilt laptops lost endpoint protection. NorthStar reinstalls the agents and wants to close the finding. The reviewer refuses because the deployment process would fail again on the next rebuild. The work package expands to update the image or automated enrollment, reconcile assets after rebuild, and alert on missing protection. Closure includes successful rebuild testing and population reconciliation. This scenario demonstrates why symptom correction is not always durable remediation.

Scenario 7: Scope reduction through a secure enclave

Management considers moving all CUI work into a dedicated enclave to reduce the number of systems requiring Level 2 controls. The roadmap treats this as an architecture program, not a documentation exercise. The team redesigns data flows, identity, remote access, administration, printing, backups, provider services, and user workflows. After migration, it validates logical and physical separation and re-runs scoping. Systems are excluded only when the technical and operational facts support exclusion.

Scenario 8: A legacy application cannot support the desired authentication model

A business-critical engineering application uses local accounts and cannot integrate with the modern identity provider. Management has several choices: isolate the application and tightly control access, add an approved gateway, upgrade or replace the application, or redesign the workflow. The roadmap should compare security outcome, cost, schedule, supportability, and operational impact. Temporary

restrictions may reduce exposure, but the long-term target state needs an explicit executive decision rather than an indefinite exception.

Scenario 9: Backups succeed, but restore tests fail

Backup jobs show green status every night. During remediation validation, the team discovers that an application restore is incomplete because a dependent configuration database was omitted. The finding remains open. The durable correction updates backup scope, dependency documentation, restore procedure, and business validation. Future testing includes complete application recovery rather than isolated file restoration. The backup dashboard now includes unresolved restore-test failures, not only job success.

Scenario 10: The MSP agreement does not fund recurring evidence work

NorthStar helped Harbor Point prepare for the assessment and manually assembled quarterly evidence. The service agreement, however, covers only ordinary IT support. The roadmap identifies that recurring access reviews, evidence exports, and validation require funded service ownership. Harbor Point can amend the agreement, perform the work internally, automate portions, or select another service model. The control should not depend on unpaid discretionary labor that may disappear after the readiness project.

Scenario 11: Too many remediation projects compete for one maintenance window

Identity changes, firewall segmentation, application updates, and endpoint baseline changes all require weekend work. The roadmap shows that forcing them into the same window increases rollback complexity and makes validation ambiguous. Management sequences foundational identity and network changes first, then validates applications, then deploys endpoint hardening. Dependency mapping preserves the reason for the order. The goal is not fastest activity but safest transition to the target state.

Scenario 12: Closed findings keep coming back

Harbor Point notices that several previously closed access and patch findings reappear after personnel changes and new systems. The remediation office treats recurrence as a program finding. It adds lifecycle triggers, population reconciliation, recurring reviews, and change-driven checks. The metric shifts from number of findings closed to repeat-finding rate and time to detect drift. Sustainable readiness

improves because the organization now monitors the conditions that create the gap, not only the gap itself.

Review Questions

1. Why is a gap finding not the same thing as a remediation plan?

2. What is the difference between containment, correction, and prevention?

3. Why should the original finding and evidence be preserved after remediation begins?

4. How does root-cause analysis reduce repeat findings?

5. What information should a remediation work package contain?

6. Why should related findings be clustered before implementation?

7. How can a tool-first remediation strategy increase scope or operational complexity?

8. What factors should influence remediation priority?

9. Why are remediation waves more useful than one final deadline?

10. What kinds of dependencies should be tracked explicitly?

11. Why should each work package have one outcome owner?

12. How does decision authority differ from technical execution?

13. Why must business disruption be considered during security remediation?

14. How should temporary protections be represented in the roadmap?

15. What recurring problem does inventory-to-console reconciliation solve?

16. Why does a successful patch deployment not necessarily close a vulnerability finding?

17. How should provider evidence limitations be remediated?

18. When can scope reduction be a valid remediation strategy?

19. Why should training and user adoption be part of technical remediation?

20. What is the difference between an internal corrective-action register and formal POA&M status?

21. Why should closure criteria be defined before implementation?

22. How does change management support remediation quality?

23. Why should remediation be independently validated when practical?

24. What should closure evidence demonstrate?

25. What makes a remediation sustainable after the project ends?

26. Why should total remediation cost include recurring operations?

27. How can capacity constraints invalidate an otherwise reasonable roadmap?

28. Which metrics provide better insight than ticket closure count?

29. What should be included in an executive remediation decision package?

30. How does the Harbor Point case study show the difference between closing a task and closing a finding?

Answer Guidance

Questions 1 through 7 focus on remediation design. The organization should preserve the original finding, identify root cause, define a target state, and package related work around an outcome rather than a collection of unrelated tickets or tool purchases.

Questions 8 through 14 focus on sequencing and governance. Priority should reflect security significance, breadth, dependency, and timing. Work should be grouped into waves, with explicit dependencies, one outcome owner, decision authority, business impact, and interim protections.

Questions 15 through 19 focus on operational patterns. Coverage, vulnerability, provider, scope, and training problems require repeatable processes and validation. Corrective work should change the operating system that produced the finding, not only the visible symptom.

Questions 20 through 25 focus on closure discipline. Internal corrective tracking is broader than formal POA&M treatment. Closure criteria, controlled change, independent challenge, evidence, and sustainment distinguish completed security outcomes from optimistic project status.

Questions 26 through 30 focus on management. Remediation requires realistic cost and capacity, outcome-focused metrics, explicit executive decisions, and evidence that the original condition has actually been corrected.

Key Terms

Term	Meaning in this chapter
Remediation roadmap	The sequenced program that converts verified findings into implemented, validated, documented, and sustainable corrections.
Work package	A controlled unit of remediation organized around one defined security outcome.
Containment	Immediate action that reduces exposure while durable remediation is being developed.
Correction	Action that fixes the verified condition.
Prevention	Process or architecture change intended to reduce recurrence.
Root cause	The underlying governance, process, architecture, responsibility, technical, or resource condition that produced the finding.
Dependency	A prerequisite action, decision, resource, provider response, or technical state needed before work can proceed.
Outcome owner	The role accountable for carrying a work package through validated closure.
Closure criteria	Predefined conditions and evidence that demonstrate the remediation achieved its target state.
Re-test	Assessment performed after implementation to determine whether the original finding is resolved.
Corrective-action register	Internal tracking record for known weaknesses and remediation regardless of formal POA&M eligibility.
Remediation wave	A management grouping of work based on risk, dependency, resources, and execution sequence.
Interim protection	Temporary risk-reduction measure used while durable remediation is pending.
Sustainment	Recurring ownership, monitoring, review, and maintenance that keeps the corrected state operating over time.

Closing Perspective

A strong remediation roadmap changes the organization, not just the spreadsheet. It removes unnecessary access, restores control coverage, clarifies authority, repairs evidence processes, reconciles providers, improves architecture, and makes recurring security work sustainable. The roadmap is successful when the environment is demonstrably stronger and the people operating it understand what must continue.

For an MSP, remediation is also a service-design exercise. Every new recurring review, escalation path, evidence export, technical control, or after-hours responsibility must be incorporated into tooling, staffing, contracts, and governance. Otherwise the readiness project creates obligations that ordinary service delivery cannot maintain.

Harbor Point now has a defensible sequence from discovery to implementation: identify the information, define the scope, assign responsibility, perform the gap assessment, and remediate the verified weaknesses. The next chapter should build on this work by organizing the evidence and operational records needed to demonstrate sustained implementation and prepare the organization for assessment activity without turning evidence collection into a last-minute scramble.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. Use the current provisions for assessment, POA&M, affirmation, scoping, and external service providers.

R2. National Institute of Standards and Technology. NIST SP 800-171 Revision 2 and NIST SP 800-171A (June 2018), as used by the published Level 2 framework discussed in this book.

R3. Office of Industrial Base Growth, July 13, 2026. Forging the Arsenal of Freedom: Department Suspends CMMC Phase II Requirements. Phase I self-assessment requirements remain in place while the Department conducts a broader program review; underlying safeguarding obligations continue.

R4. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Review the current clause and the customer’s actual contract for applicable requirements.

R5. Current Department CMMC resources, FAQs, and acquisition guidance. Confirm current program status before relying on transition dates or assessment requirements.

Sources reviewed September 19, 2026. The roadmap structures and examples in this chapter are educational management methods. They do not replace the governing regulation, contract, legal advice, or an authorized CMMC assessment.

CMMC for MSPs

From Readiness to Certification

Chapter 9

Building the CMMC Evidence Package and Assessment Readiness

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and source context

9.1–9.8 Evidence architecture and evidence-quality foundations

9.9–9.16 Evidence repositories, indexing, retention, and chain of custody

9.17–9.23 MSP/provider evidence boundaries and cloud evidence

9.24–9.30 Assessment preparation, interviews, demonstrations, and logistics

9.31–9.36 Evidence packages for the 14 Level 2 families

9.37–9.41 Harbor Point evidence-readiness case study

9.42–9.46 Sustainment, dashboards, common failures, and chapter review

Key terms and official references

Chapter Purpose

After an organization defines scope, assigns responsibility, performs a gap assessment, and remediates verified weaknesses, it still faces a practical question: can it demonstrate what it has implemented without reconstructing months of history under pressure? Chapter 9 addresses that question. Evidence is the bridge between a control that people believe exists and an implementation that can be examined, explained, and tested.

For an MSP, evidence readiness is a service-delivery issue rather than a filing exercise. The same ticketing system that records a privileged access change, the same RMM console that shows endpoint coverage, the same SOC workflow that tracks an alert, and the same identity platform that logs authentication may become important sources of evidence. If those records are incomplete, mixed across customers, unavailable after a retention period, or dependent on one technician's personal knowledge, the customer may have difficulty demonstrating sustained implementation even when much of the underlying security work is sound.

This chapter develops an evidence architecture for CMMC readiness. It explains how to identify authoritative evidence sources, connect artifacts to assessment objectives, manage evidence custodianship, build a usable index, preserve attribution, protect sensitive evidence, and prepare for interviews and demonstrations. It also examines the boundaries between customer evidence and provider evidence so that shared or inherited responsibilities are demonstrated without overstating what an MSP or cloud provider can prove for the customer.

The goal is not to create a giant static binder. A mature evidence program uses normal operations to produce reliable records, then organizes those records so they can be retrieved, explained, and validated. Harbor Point Engineering, NorthStar Managed Technology, and Beacon SOC continue as the book's fictional case study to illustrate how evidence readiness can become part of ongoing service delivery rather than a last-minute assessment project.

Learning Objectives

- Distinguish operational records, assessment evidence, management records, and narrative documentation.
- Identify authoritative evidence sources for security requirements and assessment objectives.

- Evaluate evidence for relevance, attribution, completeness, currency, authenticity, and consistency.
- Design an evidence index that connects artifacts to scope, responsibilities, objectives, time periods, and custodians.
- Establish secure evidence repositories, retention rules, access controls, and transfer processes.
- Explain how MSP, MSSP, CSP, and other provider evidence should be connected to the customer implementation.
- Prepare personnel for assessment interviews and demonstrations without scripting artificial answers.
- Build family-level evidence packages that support examine, interview, and test activities.
- Maintain readiness through recurring evidence refresh, control monitoring, and change triggers.

Source and Applicability Note

This chapter uses the published CMMC framework in 32 CFR Part 170 and the Level 2 requirement baseline in NIST SP 800-171 Revision 2. The assessment discussion refers to NIST SP 800-171A (June 2018) for the applicable Revision 2 assessment objectives and examine, interview, and test methods. Internal evidence architecture should be tied to the exact requirement and assessment sources incorporated by the applicable rule and contract rather than to a generic compliance checklist. [R1, R2, R3]

As of September 2026, the Department announced on July 13, 2026 that the transition to CMMC Phase II requirements was suspended while Phase I self-assessment requirements remain in place and the program undergoes review. The Department also emphasized that underlying contractual safeguarding obligations remain. This chapter therefore treats evidence readiness as an operational cybersecurity discipline that remains useful regardless of acquisition timing and that should be aligned to the customer’s current contractual requirements. [R4]

Evidence retention periods, legal holds, incident-preservation requirements, contract requirements, provider-service limits, and assessment-artifact rules are not identical. The examples in this chapter are management methods unless a cited source states

otherwise. Organizations should determine each retention obligation from its governing source rather than assuming that one universal period applies to every log, ticket, screenshot, report, or assessment artifact.

9.1 Evidence Is the Record of a Working Security Program

Evidence should emerge from the way the organization performs security work. When an account is approved, the approval record exists because the business decision was made. When NorthStar changes a firewall rule, the change record exists because the organization controlled the configuration. When Beacon investigates an alert, the case record exists because the monitoring process required analysis and disposition. These records have operational value before anyone labels them assessment evidence.

A weak readiness program reverses this relationship. It waits until assessment preparation and then asks technicians to create screenshots that prove controls exist. That approach may capture the current screen but miss the history, authorization, exception handling, and recurring operation that the assessment objective requires. It also encourages one-time demonstrations that are difficult to sustain.

The evidence program should therefore answer two questions continuously: what record does this control naturally produce when it operates correctly, and where will that record be retained so that the right people can retrieve it later? Those questions should be part of control design and service design rather than a separate documentation project.

For MSPs, the distinction is especially important because service platforms frequently overwrite or age out detailed operational data. If a customer needs to rely on historical tickets, authentication logs, scan reports, backup results, or alert records, the service arrangement should account for retention, export capability, and customer-specific attribution before the history disappears.

Evidence readiness begins when the control is designed, not when the assessor asks for a file.

9.2 Separate Four Kinds of Records

Evidence programs become confusing when every document is placed in one folder called CMMC Evidence. Harbor Point separates four categories: narrative

documentation, operational records, governance records, and assessment-preparation artifacts. Each category serves a different purpose.

Narrative documentation includes the SSP, policies, procedures, diagrams, inventories, and responsibility descriptions. Operational records show that work occurred: tickets, logs, approvals, scan results, access reviews, training completion, backup results, and incident cases. Governance records show oversight and decisions: exception approvals, risk decisions, management reviews, supplier reviews, and remediation prioritization. Assessment-preparation artifacts organize and explain these sources without replacing them.

A readiness worksheet may point to a privileged-access review, but the worksheet is not the review itself. A slide describing the network boundary is not the authoritative firewall configuration. A spreadsheet listing closed vulnerabilities is not equivalent to the scanner result and rescan evidence that support closure. The evidence index should preserve these distinctions.

Record type	Primary purpose	Examples
Narrative documentation	Describe the environment and process	SSP, policy, procedure, diagram, inventory
Operational record	Show activity or system state	Ticket, log, access export, scan result, backup report
Governance record	Show oversight, authorization, or risk decision	Exception approval, management review, supplier decision
Assessment-preparation artifact	Organize and explain evidence	Evidence index, interview map, demonstration plan

9.3 Start with Assessment Objectives, Not File Names

The best evidence architecture is objective-driven. Instead of collecting documents by department and hoping they later map to requirements, the team identifies the fact that must be determined and then records which evidence sources can support that fact. This mirrors the objective-level discipline introduced in Chapter 7.

For each objective, Harbor Point’s evidence index records the authoritative source, supplemental sources, responsible custodian, relevant population, period covered, and expected refresh trigger. An objective may require several sources. A privileged-access objective may rely on role configuration, approved access records, authentication logs, review results, and an interview with the identity administrator.

One artifact can also support several objectives. A current asset inventory may contribute to endpoint coverage, vulnerability management, malicious-code protection, backup scope, and configuration monitoring. The evidence program should reference the same authoritative inventory rather than creating five slightly different spreadsheets that drift apart.

This approach reduces evidence volume while improving traceability. The question becomes what does this artifact prove and which objectives rely on it? rather than how many files have we collected?

9.4 Evaluate Evidence Quality Before Calling It Evidence

An artifact should be evaluated for relevance, attribution, completeness, currency, authenticity, consistency, and retrievability. A screenshot can be genuine and current but still fail to show which tenant or customer it represents. A quarterly access review can be complete but inconsistent with the actual privileged group membership. A provider report can be authoritative for the provider’s service yet irrelevant to a customer-side responsibility.

Harbor Point uses a simple evidence-quality review before adding a source to the evidence index. The reviewer records what the artifact demonstrates, what it does not demonstrate, the period covered, the environment represented, and any dependencies or assumptions. This prevents future reviewers from overreading a familiar artifact.

Currency depends on the claim. A network diagram created six months ago may still be accurate if no material changes occurred and the organization can substantiate that fact. A current authentication screenshot may be insufficient for a claim about sustained MFA coverage over the prior quarter. Evidence freshness should therefore be evaluated relative to the objective and operating process, not through an arbitrary universal age limit.

Quality dimension	Question
Relevance	Does the artifact address the fact that must be determined?
Attribution	Can it be tied to the correct customer, system, user, tenant, or process?
Completeness	Does it represent the relevant population or clearly state its limits?
Currency	Is the time period appropriate to the claim?
Authenticity	Is the source trustworthy and traceable?
Consistency	Does it agree with other authoritative records and the actual environment?

Retrievability	Can an authorized person obtain it again through the normal process?

9.5 Use Source Evidence and Presentation Evidence Deliberately

Source evidence is generated by the system or process that performs the work. Presentation evidence is created to make that source easier to understand. A raw identity export may be source evidence; a summarized table showing privileged roles may be presentation evidence. Both can be useful, but they should not be confused.

Presentation evidence can improve assessment efficiency when complex records need context. NorthStar may prepare a customer-specific report that explains which RMM role grants what capability and then attach the authoritative role export. Harbor Point may prepare a network boundary diagram and retain the underlying firewall configuration and approved connection records. The summary helps the reviewer; the source supports the facts.

Problems arise when a summary replaces the underlying record. A polished dashboard can hide missing assets, failed jobs, or excluded accounts. The assessment team should know how the dashboard was produced, what population it covers, and whether the underlying data remains available for follow-up.

9.6 Build Evidence Around Populations and Samples

Many security processes operate over a population: all in-scope endpoints, all privileged users, all terminated personnel, all required log sources, all vulnerability findings, or all training participants. Evidence should make the population visible before the team selects representative examples.

A single successful termination ticket may show that one workflow operated correctly. It cannot establish whether the same process covered every termination during the period. A vulnerability report with hundreds of findings may show that scanning occurred but not whether the scanner covered every expected asset. The evidence program should therefore distinguish population evidence from sample evidence.

Population evidence helps define completeness. Sample evidence provides depth. Harbor Point may reconcile its current privileged-user population, then select a few access grants, modifications, reviews, and removals to demonstrate lifecycle behavior. This is more informative than collecting dozens of unrelated screenshots.

9.7 Make Evidence Time-Aware

Security controls operate through time. The assessment team needs to know whether an artifact is a point-in-time configuration, a recurring process record, a historical activity record, or a current population snapshot. The evidence index should record that distinction.

A firewall configuration export shows state at a moment. A change ticket shows how one rule changed. A monthly rule review shows recurring oversight. An authentication log shows activity during a period. Together they can tell a stronger story than any one source alone.

Evidence time awareness also helps with retention planning. If the organization needs to demonstrate quarterly access review, retaining only the current membership export is insufficient. If it needs to demonstrate restoration testing, backup job history may not be enough without the test record and business validation. The evidence plan should follow the lifecycle of the control.

9.8 Protect the Evidence Repository as a Security Asset

Evidence can contain sensitive information about identities, vulnerabilities, network architecture, incident activity, cryptographic configuration, administrative access, and control weaknesses. Collecting evidence into one repository can therefore create a concentrated target.

Harbor Point restricts evidence access by role, logs repository access, encrypts transfer and storage as appropriate, avoids unnecessary duplication, and separates customer-specific material from other NorthStar customers. The team also identifies evidence that contains CUI, Security Protection Data, personal information, or other sensitive content and applies the appropriate handling rules.

The repository should not become a shadow system that bypasses normal retention, incident, access, and disposal processes. Evidence copies need owners, purpose, retention, and deletion rules. When the authoritative record can be retrieved reliably from the source system, the evidence index may reference that source rather than duplicating the entire record population.

9.9 Design the Evidence Index

The evidence index is the navigation layer between requirements, responsibilities, and authoritative records. It should allow a reviewer to move from an objective to the

person who can explain it, the record that supports it, and the system where that record originates.

Harbor Point avoids a flat list of filenames. Each evidence entry identifies the requirement or objective, control owner, evidence source, custodian, repository, period covered, relevant scope, refresh trigger, sensitivity, and retrieval instructions. Provider evidence also identifies the exact service offering and the customer responsibility it supports.

The index is a living control record. When NorthStar changes its identity platform, the evidence source may change. When a provider revises its customer responsibility matrix, the reference may need updating. When a new remote-work location enters scope, the evidence population may expand.

The evidence index should be understandable to someone who did not build it. If the only useful retrieval instruction is ask Steve, the evidence process depends on tribal knowledge rather than a controlled system.

Field	Example
Objective	3.5.3[a] or the applicable objective identifier
Implementation owner	NorthStar Identity Team
Authoritative source	Identity platform policy export
Supplemental evidence	Privileged role report, exception register, auth log sample
Population / scope	Harbor Point privileged identities
Period covered	Quarter or point-in-time, as applicable
Custodian	Customer evidence coordinator
Location	Restricted evidence repository / source-system link
Refresh trigger	Quarterly and after material identity change
Sensitivity	Restricted technical/security information

9.10 Use Naming Conventions That Preserve Context

A naming convention should help people understand the artifact without turning filenames into overloaded databases. Useful elements can include customer identifier, control family or objective, artifact type, system, period, and version. The exact pattern matters less than consistency.

For example, HPE_AC_PrivilegedAccessReview_2026Q3_v1 communicates more than Final_Access_List_New.xlsx. NorthStar also avoids embedding secrets, passwords, CUI markings, or personal data unnecessarily in filenames because filenames are often visible in logs, sync clients, and search interfaces.

Versioning should distinguish approved records from drafts. If a policy or SSP is revised, the evidence package should identify the version that applied during the period under review and the version that applies now. Replacing the old file without preserving the relevant history can destroy context.

9.11 Separate Authoritative Repositories from Assessment Copies

Not every artifact should be copied into the assessment folder. The ticketing platform may remain the authoritative source for support records. The identity platform may remain authoritative for role membership. The evidence package can contain controlled exports or links when needed for assessment while the source system remains the system of record.

This reduces duplication but requires reliable access. If the provider portal retains data for only thirty days, a pointer is not enough for a process that depends on older history. The evidence architecture should identify which records must be exported or archived and which can remain in place.

Assessment copies should preserve context. An exported CSV without the query criteria, tenant, timestamp, or population definition may be difficult to interpret later. NorthStar records how the export was generated and, where useful, stores a readme or evidence note that explains the source and limits.

9.12 Establish Evidence Custodianship

The person who performs the security work is not always the person who should manage the assessment evidence. A SOC analyst may investigate alerts, while the evidence custodian ensures that the relevant case records can be retrieved. An HR manager may initiate termination, while the identity team retains the access-revocation record.

Harbor Point’s responsibility matrix therefore includes evidence custody where it matters. The custodian does not change the underlying control ownership. The role ensures that records are preserved, protected, indexed, and retrievable. A backup custodian is identified for critical evidence sources so that readiness does not depend on one employee’s availability.

Provider evidence custody should also be explicit. If Beacon can produce monthly reports only through a customer portal, Harbor Point identifies who downloads or

archives them. If NorthStar owns the ticketing platform, the service agreement should establish what evidence can be delivered to the customer and under what conditions.

9.13 Define Retention by Record Type and Governing Source

Retention should be determined record by record. Operational logs may have one retention requirement, incident evidence another, assessment artifacts another, personnel records another, and contractual records another. Organizations should not treat an assessment-related retention rule as a universal rule for every security record.

Harbor Point’s retention matrix identifies the record category, governing source, minimum period, business need, system limitation, custodian, and deletion or archive method. When a provider service offers less retention than the customer needs, the remediation options include changing service tier, exporting records, adjusting architecture, or revising the control design.

Legal hold, incident preservation, investigation, or contractual obligations can supersede ordinary deletion schedules. The evidence program should be able to suspend normal disposition when an authorized hold applies.

9.14 Maintain Integrity and Traceability of Assessment Artifacts

Internal readiness evidence should be protected from casual editing. Where practical, preserve source exports, timestamps, signatures, system-generated identifiers, hashes, or other traceability indicators appropriate to the artifact. The goal is not to build a forensic chain of custody for every screenshot. The goal is to preserve confidence that the reviewed artifact is the one generated by the described system or process.

When a screenshot is used, capture enough context to identify the system, tenant, relevant configuration, and date without exposing unnecessary secrets. Avoid cropping away the very details needed to establish attribution. If redaction is necessary, document what was removed and retain the authorized source when appropriate.

Evidence notes should distinguish reviewer annotations from original records. A readiness analyst can add comments explaining why an artifact matters, but those comments should not be confused with the source system’s output.

9.15 Use Evidence Notes to Explain Complex Artifacts

Some evidence is difficult to interpret without context. A firewall export may contain hundreds of rules. A vulnerability report may include systems outside the CMMC scope. A cloud configuration export may use vendor-specific terminology. Evidence notes can explain which part supports the objective, what scope filters were applied, and what limitations remain.

A strong evidence note is short and factual. It identifies the source, generation method, relevant scope, time period, and why the artifact matters. It does not make unsupported conclusions such as this proves the control is fully compliant. That judgment belongs in the assessment working record and should consider all relevant evidence.

Evidence notes also support continuity. Months later, a different engineer can understand why a particular export was retained and how to reproduce it. This reduces dependence on memory and speeds recurring reviews.

9.16 Test Retrieval Before the Assessment

Retrieval should be rehearsed. Harbor Point selects representative evidence from several families and asks the assigned custodian to produce it using normal access. The team records how long retrieval takes, whether permissions are correct, whether the record is attributable, and whether the file can be explained without the original technician present.

This exercise often reveals hidden weaknesses: expired portal accounts, provider reports that cannot be exported, filenames that cannot be tied to the correct period, archives that only one engineer can access, and records that require manual reconstruction. These are evidence-system gaps even when the underlying control may be working.

The retrieval test should include at least one provider-dependent artifact and one historical artifact. Current screenshots are usually easy to obtain. Historical provider records are where readiness problems often appear.

9.17 Define the Customer-MSP Evidence Boundary

The customer’s evidence package should not become a dump of the MSP’s internal environment. It should include the customer-specific facts needed to support the implementation and the agreed provider contribution. NorthStar may have internal

workforce records, other-customer data, proprietary automation, and sensitive architecture that are not necessary or appropriate to disclose.

The responsibility matrix helps identify the evidence boundary. If NorthStar performs endpoint configuration, the customer may need configuration outputs, coverage reports, exceptions, change records, and personnel explanation sufficient to support the relevant objectives. Harbor Point does not automatically need every internal NorthStar administrative record.

The service agreement should support this evidence relationship. If the customer relies on a provider action but the provider refuses to provide any evidence or explanation of that action, the design may be difficult to substantiate. This should be discovered during service selection and readiness, not on assessment day.

9.18 Protect Other Customers When Producing MSP Evidence

Multi-tenant MSP platforms create a confidentiality challenge. Screenshots, exports, dashboards, and ticket reports may show information about several customers. NorthStar should use customer-scoped views, filtered exports, or other controlled methods that demonstrate Harbor Point’s configuration without disclosing unrelated data.

Redaction can help, but excessive redaction can destroy attribution. The evidence process should prefer source-system filtering where possible. If the platform cannot produce customer-specific records, that limitation should be evaluated as part of service suitability and evidence design.

Provider technicians should also avoid copying multi-customer evidence to unmanaged local devices for editing. Evidence preparation should occur through controlled workflows that preserve access logging and customer separation.

9.19 Collect Provider Evidence at the Exact Offering Level

A provider’s certificate, authorization, assessment report, or compliance statement is useful only when it applies to the service offering, tenant, region, and conditions the customer actually uses. Vendor brand recognition does not establish the scope of the provider assurance.

Harbor Point’s provider evidence record identifies the legal entity, service name, offering or tier, region, relevant assurance artifact, current version or date, customer

responsibilities, and any configuration prerequisites. The record also notes which customer objectives rely on the provider contribution.

When provider documentation changes, the custodian reviews whether Harbor Point's implementation or SSP is affected. Downloading a provider responsibility matrix once and storing it indefinitely is not a complete evidence process.

9.20 Handle Cloud Evidence Through Shared Responsibility

Cloud evidence should follow the service model. The provider may supply assurance for infrastructure and platform responsibilities while the customer must demonstrate tenant configuration, identity, logging, access, information handling, and enabled features. NorthStar may perform some of those customer-side tasks under its managed-service agreement.

The evidence package should make these layers visible. A provider assurance artifact supports the provider contribution. A tenant configuration export supports the customer-side configuration. A NorthStar change ticket supports the implementation activity. A Harbor Point approval supports the business decision. Together they tell the shared-responsibility story.

Do not treat a provider's assurance as a universal replacement for customer evidence. The fact that the platform can enforce MFA does not show that Harbor Point enabled it for the required population. The fact that the provider maintains physical controls does not show how printed CUI is protected in the Harbor Point office.

9.21 Treat Security Protection Data as Sensitive Evidence

Evidence repositories frequently contain Security Protection Data: vulnerability findings, network diagrams, security configurations, logging information, detection rules, asset details, and other data associated with security functions. Even where an artifact is not CUI, it can provide significant value to an attacker.

NorthStar classifies evidence by sensitivity and limits distribution accordingly. Customer-facing evidence packages should exclude secrets such as passwords, private keys, tokens, recovery codes, and unnecessary credential material. Demonstrating that a control exists should not require exposing the secret that the control protects.

When assessors or authorized reviewers need access to sensitive technical records, the exchange method should be approved, logged, and limited to what is necessary. Temporary assessment workspaces should have closure and disposal procedures.

9.22 Use Provider Attestations Carefully

A provider attestation can support a fact that the provider is uniquely positioned to know, but it should not be used as a blanket replacement for technical evidence when technical evidence is available. The attestation should identify the service, responsibility, period, conditions, and authorized signer.

For example, a provider may attest to a personnel-screening process or a facility practice that the customer cannot directly inspect. Harbor Point should understand what assurance supports the statement and whether the provider commitment is contractual. A generic sales letter stating that the company follows best practices is weak evidence.

The customer should also avoid writing attestations on behalf of the provider. If NorthStar performs the activity, NorthStar should supply the relevant evidence or authorized statement. Harbor Point should not transform an assumption into evidence by repeating it in the SSP.

9.23 Plan for Provider Change and Evidence Portability

Evidence continuity matters when a customer changes MSPs, SOC providers, cloud platforms, or service tiers. Historical records may be needed after the provider relationship ends. The transition plan should identify which records must be exported, how they will be protected, and who retains authorized access.

Harbor Point’s offboarding checklist includes current configurations, open findings, ticket history relevant to assessment, incident records, access reviews, backup validation records, provider responsibility documents, and any customer-specific evidence index maintained by NorthStar.

A provider transition should not erase the organization’s security history. The customer may choose to retain only records justified by applicable requirements and business needs, but the decision should be deliberate rather than the accidental result of account termination.

9.24 Prepare for Assessment as an Operational Demonstration

Assessment preparation should not be a theater production. The organization should be ready to show how ordinary work occurs, identify the records that support it, and explain where provider responsibilities begin and end. The assessment team should know who can demonstrate each system and who can speak to authorization, governance, and business context.

Harbor Point creates an assessment map that lists requirement families, likely interviewees, technical demonstrators, evidence custodians, provider contacts, and backup personnel. This does not script assessor questions. It ensures that the right people are available and that no critical control depends on a single unavailable employee.

The readiness team also verifies that demonstrations can be performed safely. Production systems may require change windows or read-only access. Sensitive consoles may need screen-sharing controls. Test accounts and approved sample data may be appropriate for certain demonstrations.

9.25 Prepare Interviewees Without Coaching Answers

Interview preparation should focus on understanding, not memorization. Personnel should know their role, the workflow they perform, the systems they use, the approvals they rely upon, and the records they produce. They should be comfortable saying when another role owns a decision.

NorthStar does not give technicians a script of requirement language. Instead, it walks through real events: onboarding, privileged access, failed patching, an alert, a restore request, a configuration change, or a provider escalation. The technician explains what happens and where the evidence is created.

If different people describe different workflows, the organization should reconcile the process before assessment rather than training everyone to repeat one sentence. Consistent understanding should emerge from a consistent operating process.

9.26 Prepare Technical Demonstrations Around Questions

A demonstration should have a purpose. Before opening a console, identify what fact the reviewer needs to observe. For MFA, the demonstration may show the policy assignment, relevant user population, and authentication behavior. For logging, it

may show a source generating an event and the event arriving in the monitoring platform.

Demonstrators should avoid wandering through unrelated settings. Too much console navigation can expose secrets or unrelated customer information and can confuse the assessment story. A focused path supported by source evidence is usually stronger.

If a control depends on automation, show the relevant automation configuration and how failures are detected. If a control depends on a provider, show the provider's contribution and the customer-side prerequisites. The demonstration should align with the documented implementation.

9.27 Create an Assessment-Day Evidence Workspace

A temporary assessment workspace can improve organization, but it should be controlled. Harbor Point creates a read-only or tightly managed workspace containing approved evidence copies, the evidence index, current SSP, scope records, responsibility matrix, diagrams, and provider documentation. Access is limited to authorized participants.

The workspace is not the only evidence source. If the reviewer requests deeper source-system evidence, the custodian retrieves it through the normal process. The workspace provides efficiency without creating the false impression that every possible artifact was preselected.

After the assessment or review, temporary copies are reconciled with retention and disposal requirements. Sensitive records should not remain indefinitely in ad hoc collaboration folders created only for assessment convenience.

9.28 Manage Questions, Follow-Ups, and Evidence Requests

Assessment activity often creates follow-up questions. Harbor Point assigns one coordinator to record requests, owners, due dates, evidence delivered, and open issues. This reduces duplicate responses and prevents one technician from giving an unofficial answer that conflicts with another team's records.

The coordinator should not filter facts to make the organization look better. The role organizes communication and preserves traceability. When an answer is uncertain, the team records the question and investigates. Guessing under pressure can create contradictions that are harder to resolve than a careful follow-up.

Provider follow-ups should be tracked separately when they depend on external response times. If a provider cannot deliver evidence promptly, the limitation should already be known from readiness testing rather than discovered for the first time during the assessment.

9.29 Handle Contradictory Evidence Transparently

Contradictions occur. A ticket may say an account was disabled on Monday while the identity log shows successful authentication on Tuesday. A diagram may show one remote-access path while a technician demonstrates another. A provider report may list a retention period different from the SSP.

The readiness team should investigate the contradiction rather than selecting the artifact that supports the preferred conclusion. Determine which source is authoritative, whether the control failed, whether documentation is stale, and whether the discrepancy affects other objectives.

Harbor Point maintains a contradiction log during preparation. Significant issues become findings or remediation actions. Minor clerical inconsistencies are corrected with version control. The key is that evidence quality improves through reconciliation, not through selective presentation.

9.30 Separate Readiness from Assessment Outcome

A well-organized evidence package increases readiness, but it does not guarantee an authorized assessment outcome. The assessor may select different samples, ask different follow-up questions, observe a changed system state, or interpret evidence differently within the governing methodology.

NorthStar therefore describes its service as evidence preparation, readiness support, and implementation documentation. It does not promise that the customer will pass. This protects the integrity of the work and keeps the focus on demonstrable security rather than a sales guarantee.

The customer should also avoid treating the evidence package as a substitute for ongoing operation. A beautifully organized folder becomes stale quickly if access changes, providers update services, logs stop flowing, or policies no longer match reality.

9.31 Access Control Evidence Package

Access Control evidence should connect authorized need to implemented permissions and ongoing review. Harbor Point maintains population evidence for users, privileged users, service accounts, remote access, and relevant application roles. It then links representative approvals, changes, reviews, and removals to those populations.

For MSP access, the evidence package should distinguish customer identities from NorthStar technician identities and show how provider access is authorized, strongly authenticated, attributable, reviewed, and removed. Shared support groups should be documented at the customer-impact level rather than hidden inside the MSP’s internal organization.

- Approved access requests and manager or data-owner decisions.
- Current group, role, and privileged-access exports.
- Remote access and RMM role configuration.
- Periodic access review results and exception records.
- Termination and access-revocation examples.
- Authentication or session records showing actual use where relevant.

9.32 Awareness and Training Evidence Package

Training evidence should begin with the required population. Harbor Point compares active personnel, contractors, privileged users, and relevant provider personnel with the training requirements that apply to their roles.

A provider statement that employees receive annual security training may support part of the story, but the customer should understand whether the personnel supporting its environment are covered and whether customer-specific responsibilities require additional instruction.

- Training policy and role matrix.
- Completion reports tied to named personnel.
- New-hire or role-change training records.
- Customer-specific CUI or handling guidance.
- Overdue training reports and escalation evidence.

- Role-based security or incident-response training where applicable.

9.33 Audit and Accountability Evidence Package

Audit evidence should show coverage, configuration, protection, review, and response. The package should begin with a log-source inventory reconciled to the in-scope asset inventory and then show how events move from source to collection and review.

Beacon's customer-specific reports should identify Harbor Point without disclosing other customers. Evidence should also show what happens when a critical source stops reporting, because sustained logging depends on detection of failure as well as initial configuration.

- Log-source inventory and expected event coverage.
- Audit configuration and selected event categories.
- SIEM ingestion health and failed-source monitoring.
- Retention configuration and access controls.
- Sample audit events and privileged-activity records.
- Alert or review tickets showing analysis and disposition.

9.34 Configuration Management Evidence Package

Configuration evidence should show the approved baseline, deployed state, controlled change, and exception process. Harbor Point retains secure configuration standards and NorthStar provides customer-specific deployment or compliance outputs.

Where NorthStar uses global automation, the evidence package should identify which settings apply to Harbor Point and how customer-specific deviations are governed. A generic MSP template is not sufficient if the customer implementation differs.

- Approved baseline or secure configuration source.
- Configuration-policy exports or management profiles.
- Change tickets with approval and validation.
- Emergency-change records.
- Software inventory and prohibited-software controls.

- Exception approvals and drift-remediation records.

9.35 Identification and Authentication Evidence Package

Identity evidence should make the relevant account classes and authentication paths visible. The package should support user uniqueness, credential lifecycle, MFA, device identity, local or emergency accounts, and service identities as applicable.

The evidence package should not include passwords, secret keys, recovery codes, or tokens. Demonstrate the control without exposing the secret. For MSP technicians, show how provider identities map to human users and customer-side activity.

- Identity provider policies and MFA assignments.
- Privileged and service account inventories.
- Authentication logs or representative events.
- Authenticator enrollment and reset procedures.
- Local account reports on representative systems.
- Emergency or break-glass account governance and review.

9.36 Incident Response Evidence Package

Incident evidence should demonstrate detection, triage, authority, response, reporting decisions, preservation, recovery, and lessons learned. A plan without case records provides only part of the story.

Provider and customer records should align. If Beacon opens a SOC case and NorthStar opens a technical ticket, the evidence package should show how the two records connect and where Harbor Point management made the incident decision.

- Current incident-response plan and contacts.
- SOC escalation procedure and service description.
- Representative incident or security-event records.
- Containment authorization and action records.
- Preservation and reporting decision records.
- Tabletop exercise outputs and corrective actions.

9.37 Maintenance Evidence Package

Maintenance evidence should show who performed maintenance, how access was authorized, which tools were used, and how temporary or remote maintenance access was controlled and ended.

RMM activity can support maintenance evidence, but the customer-specific record should identify the technician and system. Shared console screenshots that cannot attribute actions to Harbor Point are weak evidence.

- Maintenance procedure and authorized tools.
- Remote-maintenance session logs.
- Temporary account or vendor access records.
- Maintenance ticket with approval and completion.
- Device repair or return handling records.
- Evidence that temporary access or tools were removed.

9.38 Media Protection Evidence Package

Media evidence should follow actual information movement across removable devices, printed material, exports, backups, and disposal. The package should show authorized use, protection, transport, sanitization, and destruction where applicable.

Support screenshots, diagnostic exports, and ticket attachments can create unplanned media or information-handling records. NorthStar should control where those artifacts are stored and when they are deleted.

- Media policy and removable-media settings.
- Approved exceptions and encrypted-device records.
- Print or physical handling procedures.
- Backup-media controls where applicable.
- Asset disposal and sanitization records.
- Destruction certificates tied to specific assets or media.

9.39 Personnel Security Evidence Package

Personnel security evidence should connect personnel events to technical and physical access changes. The strongest package traces recent hires, transfers, and terminations from HR decision to security completion.

For provider personnel, the customer may rely on NorthStar's internal personnel process. The evidence package should demonstrate enough of that process to support the customer's reliance without exposing unnecessary private employee information.

- Screening records or appropriate assurance.
- HR notification or personnel action record.
- Provisioning, role-change, and termination tickets.
- Identity and physical-access updates.
- Provider technician lifecycle evidence where relied upon.
- Verification that all relevant access paths changed.

9.40 Physical Protection Evidence Package

Physical evidence should correspond to the actual places where relevant systems, devices, media, and printed information exist. Harbor Point separates customer facilities, alternate work sites, provider facilities, and cloud-provider facilities according to responsibility.

Do not use provider data-center evidence to support a customer office requirement. Evidence should be tied to the physical boundary to which it applies.

- Authorized physical-access list.
- Visitor and escort records.
- Badge, key, or access-device lifecycle records.
- Server-room or restricted-area controls.
- Alternate-work-site requirements and acknowledgements.
- Provider assurance for provider-controlled facilities where relevant.

9.41 Risk Assessment Evidence Package

Risk Assessment evidence should show recurring risk evaluation and vulnerability-management operation. The vulnerability evidence package begins with scope and coverage rather than with the count of findings.

NorthStar should preserve enough detail to show why systems were included or excluded and how scanner failures were handled. A summary percentage is helpful only when the underlying population is understood.

- Risk assessment records and management review.
- Vulnerability scanner target and coverage reports.
- Authenticated-scan status and failed-scan handling.
- Representative findings and remediation tickets.
- Approved exceptions or risk decisions.
- Rescan evidence confirming correction.

9.42 Security Assessment Evidence Package

Security Assessment evidence should demonstrate the organization’s own assessment, corrective action, monitoring, and SSP maintenance cycle. Chapter 7 and Chapter 8 outputs become part of this package when maintained as controlled records.

Closed findings should include validation evidence. A roadmap entry marked complete without re-testing is not a strong closure record.

- Internal assessment results.
- Remediation register and POA&M records where applicable.
- Re-test or closure evidence.
- Continuous-monitoring records.
- SSP revision history and approval.
- Management review of security posture and open actions.

9.43 System and Communications Protection Evidence Package

This family’s evidence should combine architecture, deployed configuration, approved connections, encryption, and key or certificate governance. Diagrams alone are insufficient; configuration alone can be hard to interpret without the diagram.

NorthStar should include MSP administrative paths and cloud connections when they affect the assessed system. These paths are often missing from customer-facing diagrams even though they are technically significant.

- Current network and data-flow diagrams.
- Firewall, security-group, and boundary configuration.
- Remote-access and VPN settings.
- Approved external connection records.
- Encryption configuration and representative observation.
- Certificate or key inventories and lifecycle records.

9.44 System and Information Integrity Evidence Package

Integrity evidence should show flaw correction, malicious-code protection, advisory evaluation, coverage, and response to unhealthy or suspicious conditions. Population reconciliation is central.

Evidence should distinguish expected assets from reporting assets. A dashboard showing 99 percent coverage is not sufficient when the missing one percent is unknown or includes a critical server.

- Patch deployment and validation reports.
- EDR or antimalware coverage and health records.
- Approved exclusions and exception records.
- Security advisory review and applicability decisions.
- Failed deployment or unhealthy-agent tickets.
- Follow-up validation after corrective action.

9.45 Harbor Point Case Study: Build the Evidence Architecture

Harbor Point begins with the objective register created during the gap assessment and adds evidence fields rather than creating a separate compliance database. Each objective now identifies its authoritative source, custodian, scope, period, sensitivity, refresh trigger, and likely interview or demonstration owner.

NorthStar reviews its managed services to identify which evidence is generated automatically and which evidence requires deliberate capture. Endpoint coverage, patch status, authentication, backup jobs, and alert cases have system-generated records. Access approval, exception decisions, business restoration validation, and provider change review require human workflow records.

The team then identifies evidence risks. The vulnerability platform retains detailed history for a limited period, the SOC portal does not export one useful view cleanly, and the RMM system includes multi-customer dashboards. These are resolved before assessment preparation: NorthStar configures scheduled customer-scoped exports where appropriate, Beacon provides a customer-specific report, and Harbor Point updates the evidence index with retrieval instructions.

The result is not a static folder. It is a map from control operation to record source. Harbor Point can reproduce the evidence package because the operational systems continue to generate the underlying records.

9.46 Harbor Point Case Study: Rehearse Interviews and Demonstrations

Harbor Point conducts a readiness day that resembles normal assessment activity without pretending to be an authorized certification assessment. The assessment lead selects representative objectives across identity, logging, vulnerability management, incident response, configuration, and physical protection.

For each objective, the assigned person explains the workflow in ordinary language, retrieves the relevant evidence, and demonstrates the technical mechanism when appropriate. Backup personnel observe. The team records retrieval delays, contradictions, inaccessible provider records, and demonstrations that depend on production changes.

The rehearsal finds two issues. One technician can explain the RMM role model but the customer-specific privileged role export is difficult to produce. A second issue appears when the SSP says Beacon contacts Harbor Point directly for critical

incidents while the live workflow routes through NorthStar. Both issues are corrected before assessment preparation continues.

The exercise also improves confidence because personnel learn that they do not need to memorize requirement language. They need to understand the work they actually perform, the boundaries of their authority, and the evidence that work produces.

9.47 Harbor Point Case Study: Build the Assessment Workspace

Harbor Point creates a restricted assessment workspace containing the current SSP, scope package, responsibility matrix, evidence index, approved diagrams, provider responsibility documents, and selected evidence copies. The workspace also contains a request log and contact matrix.

Sensitive operational records remain in source systems unless there is a reason to copy them. Where copies are created, they are labeled with source, date, scope, and sensitivity. The workspace is backed by access logging and has a defined closure process.

The evidence coordinator tests every link and every provider portal before the readiness package is approved. A backup custodian verifies that the package does not depend on the primary coordinator’s personal account. This simple test eliminates several assessment-day risks.

Management receives a summary showing evidence readiness by family, unresolved provider dependencies, open contradictions, and remediation items. The summary is operational, not a claim of certification.

9.48 Common Evidence Failures

The most common evidence failures are predictable. The organization has screenshots but no population. It has a policy but no operating record. It has a dashboard but cannot explain the data source. It has provider assurance but not for the selected service. It has current configuration but no history. It has historical records but cannot attribute them to the customer. It has evidence but only one employee knows how to retrieve it.

Another common failure is excess evidence. Teams collect thousands of files without indexing them, making it difficult to identify which source is authoritative. Duplicate screenshots and exported reports create conflicting versions. More evidence is not automatically stronger evidence.

The corrective approach is disciplined reduction. Identify the objective, choose the strongest source, preserve supplemental context, remove unnecessary duplicates, and test retrieval. The goal is a coherent evidence story, not a digital warehouse.

- Unattributed screenshots
- Stale diagrams
- Current-only evidence for recurring processes
- Multi-customer exports with unrelated data
- Provider assurance for the wrong offering
- Missing evidence of exceptions and failures
- Evidence stored only in personal folders
- Conflicting document versions
- Ticket closure without validation evidence
- Excessive duplication with no authoritative-source designation

9.49 Create an Evidence Readiness Dashboard

Management needs a concise view of evidence readiness, but the dashboard should preserve underlying nuance. Harbor Point reports the number of objectives with identified authoritative evidence, objectives with provider dependencies, overdue evidence refreshes, failed retrieval tests, unresolved contradictions, and open evidence-related remediation actions.

The dashboard does not convert those counts into a certification probability. It helps management decide where to invest effort. A single missing provider artifact may affect several objectives and deserve more attention than ten routine evidence refreshes.

Trend information can be valuable. If retrieval time decreases, stale evidence decreases, and contradictions are resolved faster, the evidence program is becoming more sustainable. These are internal performance measures rather than official CMMC scores.

Measure	Management question
Authoritative source assigned	Do we know where the strongest evidence comes from?
Provider dependencies open	Which conclusions still rely on external information?
Evidence refresh overdue	Which records may no longer reflect current

	implementation?
Retrieval failures	Can the assigned custodian actually produce the record?
Contradictions open	Where do records disagree about implementation?
Re-test evidence missing	Which remediation items cannot yet be closed confidently?

9.50 Sustain Evidence Readiness Through Change Management

Evidence readiness must survive change. New platforms, new providers, mergers, staff turnover, remote-work expansion, cloud migrations, and service-tier changes can invalidate evidence sources even when the control objective remains the same.

Harbor Point adds an evidence-impact question to material change review: does this change alter the authoritative evidence source, custodian, retention, scope, or retrieval method? If yes, the evidence index and assessment package are updated as part of the change rather than months later.

NorthStar applies the same rule to its managed-service catalog. When it replaces an RMM, SIEM, backup platform, or vulnerability scanner, the migration plan includes customer-specific evidence continuity. Historical records needed for security or assessment are exported or otherwise preserved before the old service is retired.

9.51 Build Evidence into MSP Service Design

For MSPs, evidence readiness should be a defined service capability. Service descriptions can state which reports, logs, tickets, reviews, exports, and customer-specific records are produced; how long they are available; who can request them; and what is outside the service.

This prevents the sales team from promising evidence the service platform cannot provide. It also allows engineering to select platforms partly on their ability to support customer-specific attribution, export, retention, and auditability. Compliance becomes an architecture consideration rather than a later reporting problem.

Account management should review evidence dependencies when contracts renew or service tiers change. If a customer moves to a lower-cost platform with shorter log retention, that may affect the evidence architecture and possibly the security implementation itself.

A mature MSP can use standardized evidence patterns across customers while preserving customer-specific scope and authorization. Standardization should improve consistency, not erase the differences between customer environments.

9.52 Chapter Review and Readiness Checklist

Chapter 9 completes another stage of the readiness sequence. Harbor Point now has more than a set of controls and remediation projects. It has a repeatable way to show how the security program operates, which records support each objective, who can explain the work, how provider contributions are substantiated, and how sensitive evidence is protected.

The evidence package should remain smaller than the security program it represents. It is an index and selected set of authoritative records, not a second copy of every operational system. The strongest evidence program preserves source systems, uses controlled exports where necessary, and keeps the narrative documentation synchronized with reality.

The next chapter can move from evidence readiness into the mechanics of assessment execution: managing the assessment lifecycle, working with the assessment organization, coordinating interviews and demonstrations, responding to findings, and maintaining operational stability during the assessment period.

- Every objective has an identified evidence strategy or an explicit unresolved status.
- Authoritative sources are distinguished from summaries and presentation artifacts.
- Evidence populations and samples are clear.
- Provider evidence is tied to exact services and customer responsibilities.
- Sensitive evidence is protected and access is logged.
- Retention is based on governing source and record type.
- Custodians and backup custodians can retrieve the evidence.
- Interviewees understand their workflows without relying on scripts.
- Technical demonstrations have a defined purpose and safe method.
- Contradictory records are investigated rather than hidden.
- Evidence impact is included in material change management.

Detailed Evidence Field Guide

The following field guide deepens the chapter’s methods into practical evidence patterns that an MSP and customer can use while preparing for a Level 2-style readiness review. The examples are not mandatory artifact lists. NIST SP 800-171A

identifies potential assessment objects and methods, but the organization should select evidence that actually demonstrates its implementation. The field guide is intended to make that selection disciplined and reproducible.

Field Guide 1: Access lifecycle evidence

Start with the population of active and privileged identities. Then retain representative records for authorization, provisioning, change, periodic review, emergency use, and removal. A lifecycle package is stronger than a current group screenshot because it demonstrates both state and process.

Practical test: ask a second authorized person to retrieve the relevant record and explain what it proves, the period it covers, the population it represents, and what limitation remains. If that person cannot do so without calling the original engineer, the evidence process still depends too heavily on individual memory.

MSP consideration: determine whether the record is customer-specific, whether another customer’s information could appear, how long the source platform retains the data, and whether the service agreement supports export or delivery. These provider-side conditions should be resolved before the evidence becomes critical.

Closure criterion: the evidence pattern is considered operational when the source is known, custody is assigned, retrieval works, sensitivity is controlled, and the record can be connected to the applicable implementation and objective without inventing missing context.

Field Guide 2: Remote administration evidence

Identify every remote path used by customer users, MSP technicians, vendors, and support tools. Evidence can include policy configuration, MFA assignment, named technician roles, session logs, approval records, and exceptions. Demonstrate that remote activity is attributable and that stale access is removed.

Field Guide 3: Privileged access evidence

Privileged access should have its own evidence view because high-impact administrative identities can be hidden inside broader user lists. Maintain privileged populations, role definitions, approvals, periodic reviews, emergency-account governance, session or authentication records, and removal evidence.

Field Guide 4: Endpoint coverage evidence

Reconcile the authoritative asset inventory to endpoint protection, patching, vulnerability scanning, configuration management, and backup coverage. Store the reconciliation result and investigate every missing or unexpected asset. Coverage percentages without the denominator and exception list are weak evidence.

Field Guide 5: Logging evidence

Keep a log-source inventory, ingestion-health records, retention settings, sample events, alert rules, and tickets that show review and response. Include evidence of how failed log sources are detected and repaired, because healthy logging is a continuing condition rather than a one-time configuration.

Field Guide 6: Vulnerability evidence

Preserve the target population, scan configuration, authentication status, findings, remediation actions, approved exceptions, and rescans. When a finding closes, retain evidence that the affected condition was actually corrected rather than simply scheduled or patched.

Field Guide 7: Configuration evidence

For important baselines, retain the approved standard, deployment mechanism, current compliance or drift result, change records, and exception handling. When global MSP automation is used, capture the customer-specific policy assignment and any deviations.

Field Guide 8: Backup and recovery evidence

Backup success alone does not prove recoverability. Evidence should include protected asset coverage, job health, unresolved failures, restore test records, recovered data validation, and the business owner’s confirmation that the restored information met the intended need.

Field Guide 9: Incident evidence

Link SOC alerts, MSP tickets, customer incident decisions, containment activity, reporting decisions, evidence preservation, recovery, and lessons learned. A single incident may therefore have several authoritative records that should be cross-referenced rather than merged into one artificial document.

Field Guide 10: Physical evidence

Use authorized access lists, badge or key records, visitor records, restricted-area controls, and alternate-work-site requirements. Tie provider physical evidence only to provider-controlled facilities. Do not let data-center assurance obscure customer-office responsibilities.

Field Guide 11: Training evidence

Reconcile required training populations to active personnel and relevant provider staff. Retain role-specific requirements, completion reports, overdue follow-up, and customer-specific handling guidance. Training evidence should show both assignment and completion.

Field Guide 12: Personnel event evidence

Trace hires, transfers, terminations, and provider staff changes across HR, identity, physical access, application access, and shared-provider roles. A few complete end-to-end examples are more informative than separate screenshots from each system.

Field Guide 13: Cloud evidence

Tie provider assurance to the exact offering, region, and service model. Combine provider evidence with tenant configuration, customer-side identity, logging, encryption, and integration records. Store the provider responsibility document version used during the review.

Field Guide 14: Supplier evidence

Maintain supplier inventory, due-diligence records, contract commitments, relevant certifications or reports, provider CRMs, change notifications, and termination evidence. Supplier evidence should demonstrate ongoing governance, not merely onboarding.

Field Guide 15: Exception evidence

Every exception should identify the affected requirement or control, scope, business reason, risk, approver, expiration, compensating safeguards where relevant, and remediation plan. Expired exceptions should not remain quietly active.

Field Guide 16: Remediation closure evidence

Link the original finding to the implemented change, approval, validation method, re-test result, and document updates. Closure evidence should make it possible for another reviewer to understand why the item was considered resolved.

Field Guide 17: Evidence transfer

Define secure methods for delivering evidence to authorized reviewers. Avoid sending sensitive technical exports through uncontrolled email when a more appropriate secure transfer method is available. Track what was delivered and to whom.

Field Guide 18: Evidence redaction

Redact only what is necessary to protect secrets, other customers, or unrelated personal information. Preserve enough context for attribution. Document redactions when they affect interpretation, and retain an authorized source where appropriate.

Field Guide 19: Screenshot discipline

Use screenshots for point-in-time visual settings, not as a universal evidence format. Capture system or tenant identity, relevant setting, and date where practical. Do not expose passwords, tokens, private keys, or unrelated customer data.

Field Guide 20: Export discipline

When exporting CSV, JSON, PDF, or report files, record the query, filter, tenant, date, and population. An export that cannot be reproduced or explained months later has limited evidentiary value.

Field Guide 21: Interview support

Prepare a simple role card for each interviewee listing responsibilities, systems used, normal triggers, escalation route, and evidence produced. The card is a preparation aid, not a script. The interviewee should answer from actual practice.

Field Guide 22: Demonstration support

Prepare demonstration notes that identify the question, system, safe test method, expected outcome, and evidence captured. Avoid altering production settings merely to make a demonstration easier unless the change is separately approved.

Field Guide 23: Historical continuity

Retain records needed to show sustained operation across provider transitions, staff changes, and platform migrations. Evidence continuity should be included in decommissioning and offboarding plans.

Field Guide 24: Evidence governance

Assign an evidence-program owner, family or control custodians, backup custodians, review cadence, and change triggers. Evidence governance should be lightweight enough to sustain but formal enough to survive staff turnover.

Expanded Evidence Operations Playbook

The following playbook takes the evidence concepts in this chapter and turns them into a repeatable operating method for an MSP-supported customer. Each section is intentionally more detailed than a checklist. The purpose is to show how the evidence package should be built, challenged, refreshed, and presented so that the organization can explain sustained implementation rather than produce isolated screenshots.

The playbook assumes the customer has already completed the core readiness work from earlier chapters: information discovery, scoping, responsibility allocation, gap assessment, and remediation planning. Evidence cannot repair a weak implementation. Its job is to make the real implementation visible, traceable, and explainable.

Evidence Playbook 1: Access Control

Access Control evidence should tell the entire authorization story. The starting point is the population of identities and access paths, not the ticket queue. Harbor Point identifies workforce users, privileged users, service accounts, application roles, remote access, local administrative accounts, and NorthStar technician access. The evidence package then shows how a business need becomes a technical permission and how that permission is later reviewed or removed.

The strongest evidence pattern is a lifecycle chain. Begin with an approved request or documented entitlement model. Show the resulting account or role assignment, the group or application state after implementation, and the later review or revocation record. If the system allows direct administrator changes outside the request workflow, include records that show how those changes are monitored and reconciled.

Population evidence matters because a small number of carefully chosen tickets can hide stale or excessive access elsewhere. Harbor Point therefore reconciles current privileged groups, remote-support roles, local administrator accounts, and application administrators before selecting samples. The population becomes the denominator; the samples show process depth.

MSP evidence should preserve customer separation. NorthStar may operate one RMM across many customers, but Harbor Point should receive a customer-scoped privileged-role report, customer-specific session records, and evidence that technicians are individually attributable. A global administrator list may be relevant internally to NorthStar, but Harbor Point needs the part of the provider control that affects its environment.

The evidence coordinator should also preserve exception context. Emergency accounts, break-glass identities, temporary vendor access, and approved shared technical accounts, if any are permitted, should not disappear from the package. Each exception should show purpose, authorization, protection, review, and expiration or continuing need.

Evidence structure

Evidence layer	Typical content
Population evidence	Current users, privileged users, service accounts, remote-access population, MSP technician roles
Lifecycle samples	Grant, modify, review, revoke
Technical state	Groups, roles, access-control lists, remote paths, local administrators
Operational evidence	Tickets, approvals, session records, periodic reviews
Exception evidence	Emergency access, temporary access, approved deviations

Frequent readiness failures

- Collecting only current group screenshots.
- Ignoring local or application accounts that do not use the primary identity provider.
- Using MSP global dashboards that expose other customers.
- Keeping access reviews without evidence of corrective action.
- Showing the request but not verifying the implemented entitlement.

Assessment preparation note: the organization should be able to retrieve at least one authoritative population record and one end-to-end example for this family without rebuilding the evidence manually. If retrieval depends on a single technician, unsupported custom query, or expired provider portal, the evidence program still requires remediation.

Sustainment note: identify the event that should refresh this evidence package. Examples include quarterly review, material system change, provider change, major incident, new asset class, privileged-role change, or completion of a remediation project. Evidence should change because the environment changed, not because assessment season arrived.

Evidence Playbook 2: Awareness and Training

Training evidence must begin with the required population. Harbor Point identifies employees, contractors, privileged users, incident-response roles, and provider personnel who need particular instruction. The evidence package then reconciles assignment and completion rather than storing random completion certificates.

A learning-management export is useful only when it can be tied to active personnel and role requirements. The evidence coordinator compares the HR roster, contractor roster, privileged access population, and NorthStar support population against the training matrix. This exposes the common gap where one system shows complete training while a contractor or newly privileged administrator never entered the learning system.

Role-based training should be visible separately from general awareness. An incident coordinator may require exercises that ordinary users do not. A NorthStar technician who handles CUI-related support workflows may need customer-specific handling instructions beyond the provider’s generic annual awareness training.

Overdue training is part of the evidence story. The assessment should be able to show not only completion rates but also what happens when a person misses the deadline. Harbor Point preserves escalation records, manager follow-up, and any access restriction or corrective action required by its process.

Training evidence should remain privacy-conscious. It usually does not require storing sensitive HR details in the assessment workspace. The package can identify the person, role, assigned training, completion status, and relevant date while leaving unrelated personnel information in the authoritative HR system.

Evidence structure

Evidence layer	Typical content
Population	Active personnel, contractors, privileged users, provider support roles
Assignment	Required training by role
Completion	Named completion report
Exception	Overdue and remediation evidence
Role-based	Specialized technical or incident-response training

Frequent readiness failures

- Using percentage completion without the population.
- Excluding contractors or provider staff.
- Confusing general awareness with specialized role training.
- No evidence of overdue follow-up.
- Training record does not identify the individual or course.

Evidence Playbook 3: Audit and Accountability

Audit evidence must show that required sources generate events, events reach the intended repository, records are protected, retention is configured, and someone reviews or responds to the events that matter. A SIEM dashboard by itself does not prove this chain.

Begin with the source population. Harbor Point lists domain controllers, servers, endpoints, firewalls, cloud services, identity providers, critical applications, and MSP administrative paths that are expected to produce relevant audit records. Beacon's source-health view is then reconciled to this inventory.

The package should preserve evidence of failures as well as success. A healthy system eventually has failed collectors, stopped agents, full disks, expired credentials, or network interruptions. One of the most persuasive records is a real or tested example showing that a missing source was detected, assigned, corrected, and verified.

Retention evidence should be service-specific. If different sources have different retention or archive behavior, the evidence index should reflect that. A policy sentence saying logs are retained for a period is not sufficient if the cloud platform, endpoint console, and SOC service implement different limits.

Review evidence should connect event generation to human or automated analysis. For important alerts or periodic reviews, retain case records showing what the reviewer considered, what decision was made, and what follow-up occurred.

Evidence structure

Evidence layer	Typical content
Coverage	Expected log sources vs active sources
Configuration	Audit categories and forwarding
Health	Collector/source monitoring
Retention	Configured periods and archive
Review	Alert/case/ticket evidence

Frequent readiness failures

- No source inventory.
- Healthy dashboard hides missing systems.
- Retention policy differs from platform configuration.
- No evidence of response to failed logging.
- Provider report is not customer-specific.

Evidence Playbook 4: Configuration Management

Configuration evidence should make approved state and change visible. The organization should be able to show the baseline, the mechanism that deploys or enforces it, the current state, and how deviations or exceptions are handled.

A policy PDF is only one layer. NorthStar maps baseline statements to Group Policy, MDM configuration, RMM scripts, firewall templates, cloud policies, or other technical enforcement mechanisms. The evidence package includes enough of the deployed configuration to demonstrate that the approved standard reached the intended systems.

Change evidence should trace normal and emergency workflows. The package can include a recent approved change, implementation record, validation output, and post-change review. Emergency changes should show the retrospective approval or review required by the organization.

Drift evidence is often more valuable than a static screenshot. A compliance report showing exceptions, failed deployments, or changed settings demonstrates that the

organization can detect when systems move away from the baseline. The evidence should also show how those deviations are investigated.

Where the MSP uses global automation, customer assignment must be explicit. A script that exists in NorthStar's platform does not prove Harbor Point receives it. Preserve the customer scope, policy target, version, and any customer-specific exclusions.

Evidence structure

Evidence layer	Typical content
Baseline	Approved secure configuration
Deployment	Policy/profile/script assignment
Drift	Compliance and exceptions
Change	Approved change + validation
Exception	Documented deviation and review

Frequent readiness failures

- Baseline exists only as prose.
- Global MSP template not tied to customer assignment.
- Emergency changes lack review.
- Exceptions never expire.
- No evidence that failed deployments are investigated.

Evidence Playbook 5: Identification and Authentication

Identity evidence should show how people, services, and devices are uniquely identified and authenticated across all relevant paths. The evidence package must include the systems that do not use the primary identity provider, because those are often where weak authentication persists.

Harbor Point builds an identity inventory that distinguishes workforce accounts, privileged accounts, service identities, local accounts, application identities, devices, and emergency credentials. Each class has an owner and authentication method.

MFA evidence should combine policy configuration with observed behavior. The package identifies the user groups or roles covered by the policy and includes authentication logs or a controlled demonstration that shows enforcement. Exceptions and recovery paths receive separate review.

Credential lifecycle evidence includes enrollment, reset, recovery, revocation, and protection of authenticators. A secure login policy is incomplete if help-desk reset procedures allow weak identity verification or if emergency credentials are shared informally.

Provider identities deserve their own evidence path. NorthStar's technician identities should be unique, strongly authenticated, and mapped to customer-side activity. If an MSP service account performs automation, the evidence should show how that identity is protected, rotated, and limited.

Evidence structure

Evidence layer	Typical content
Identity population	Human, service, device, local, emergency
Policy	Authentication and MFA settings
Behavior	Authentication logs / test
Lifecycle	Enrollment, reset, revoke
Provider	Technician identity mapping

Frequent readiness failures

- MFA only on primary cloud login.
- Recovery or local paths bypass controls.
- Shared provider identities.
- Service accounts used interactively.
- No evidence of authenticator reset governance.

Evidence Playbook 6: Incident Response

Incident-response evidence should connect alert to decision. It should show detection, triage, incident declaration, containment authority, reporting decisions, preservation, recovery, and lessons learned across customer and provider boundaries.

The most useful evidence is often one complete incident or exercise record. Start with the alert or report, trace the SOC case, the MSP technical ticket, customer management decision, containment activity, communication, preservation, and final closure. Cross-reference the records rather than forcing them into one document.

After-hours evidence is important because incident workflows frequently fail when the primary contact is unavailable. Harbor Point preserves a tabletop or real event showing backup contacts and escalation.

Reporting decision evidence should distinguish security response from contractual or regulatory reporting. The technical team may identify facts, while authorized management or legal personnel determine whether a reporting trigger is met. The evidence package should show the decision path without implying that the MSP owns decisions it does not.

Provider contracts and procedures should align. If Beacon's procedure routes critical alerts to NorthStar first, Harbor Point's incident plan should describe that sequence. Contradictory evidence is itself a readiness issue.

Evidence structure

Evidence layer	Typical content
Detection	Alert / report
Triage	SOC or MSP case
Authority	Incident declaration / containment decision
Action	Containment and recovery
Reporting	Decision and preservation
Improvement	Lessons learned / corrective action

Frequent readiness failures

- Alert exists but no incident decision record.
- Customer and provider escalation procedures conflict.
- After-hours contacts not tested.
- Containment authority unclear.
- No link between lessons learned and remediation.

Evidence Playbook 7: Maintenance

Maintenance evidence should show who performed work, how access was authorized, which tools were used, and how temporary maintenance conditions were removed or closed.

Remote maintenance deserves special treatment in MSP environments because RMM tools create persistent capability. The evidence package should show technician

identity, target system, session or job history, authentication, and customer authorization model.

Vendor maintenance should be traceable even when performed under a support contract. If temporary accounts or tunnels are created, the record should include activation, monitoring, and removal.

Device repair can create data-handling risk. When systems or drives leave the controlled environment, the evidence package should show the approved process, sanitization or protection decision, and return or destruction record as applicable.

Maintenance evidence should distinguish routine automated jobs from interactive technician sessions. Both may be authorized, but they have different attribution and review needs.

Evidence structure

Evidence layer	Typical content
Authorization	Approved maintenance request
Identity	Technician/vendor identity
Session	Remote or local maintenance record
Temporary access	Creation and removal
Device handling	Repair/return/sanitization

Frequent readiness failures

- Standing vendor access.
- Shared maintenance accounts.
- Temporary tools left installed.
- No proof temporary access was removed.
- Device sent to vendor with unclear data handling.

Evidence Playbook 8: Media Protection

Media evidence should reflect where information actually leaves ordinary managed storage. Removable media, printed drawings, exports, diagnostic bundles, backup media, and failed storage devices can all create evidence needs.

Start with policy and technical restrictions, then test real workflows. If removable media is restricted, the evidence package should show endpoint configuration and

approved exceptions. If printing is permitted, show how printed sensitive material is controlled and destroyed.

Support activity is a common hidden media path. A technician may export logs, copy a screenshot, or download a diagnostic bundle to investigate a problem. NorthStar should define approved locations and deletion practices so support artifacts do not become unmanaged copies.

Sanitization and destruction evidence should be attributable to the media or asset. A generic destruction certificate is less useful if the organization cannot map the record to the drive or device that held the information.

Cloud-first organizations should still ask where users download files and how local caches are handled. The absence of formal USB drives does not mean the media problem disappeared.

Evidence structure

Evidence layer	Typical content
Controls	Device / print restrictions
Exceptions	Approved removable media
Handling	Transport/storage
Sanitization	Disposal or reuse
Support artifacts	Exports/screenshots/diagnostics

Frequent readiness failures

- Policy restricts USB but endpoint does not.
- Diagnostic exports stored in personal folders.
- Destruction record not tied to asset.
- Printed CUI handling ignored.
- Local downloads not considered media handling.

Evidence Playbook 9: Personnel Security

Personnel evidence should show that personnel events drive logical and physical security actions. The most useful package traces real hires, transfers, terminations, and provider staff changes end to end.

Select a recent termination and follow it across HR notice, identity disablement, application access, badge or key access, VPN, RMM, local accounts, and provider-specific groups. This reveals gaps that separate department reports can hide.

Transfers deserve attention because they can create privilege accumulation. The evidence package should show removal of old entitlements, not just assignment of the new role.

Provider personnel lifecycle can be challenging because the customer does not administer the provider's HR system. NorthStar can supply appropriate assurance and customer-impact evidence, such as the date a technician lost customer access, without exposing unnecessary personal details.

Emergency terminations should be tested for speed and communication. If Harbor Point expects immediate revocation but the provider process operates only during business hours, the service design and documentation should reflect reality.

Evidence structure

Evidence layer	Typical content
Hire	Screening + onboarding
Transfer	Old access removal + new access
Termination	HR trigger through all access paths
Provider	Technician offboarding assurance
Verification	Post-event access test

Frequent readiness failures

- Primary account removed but local/app access remains.
- Transfers accumulate privileges.
- Provider staff changes not reflected in customer roles.
- Badge access lags behind identity change.
- No evidence of urgent termination path.

Evidence Playbook 10: Physical Protection

Physical evidence must be tied to the facility or location it describes. Customer offices, server rooms, remote work locations, MSP facilities, and cloud provider facilities are different boundaries with different custodians.

Harbor Point maintains authorized physical access lists, visitor procedures, badge or key records, and restricted-area controls for its office. A small number of recent access changes and visitors are selected as samples.

Alternate work sites need evidence that the policy is understood and practical. The package may include remote-work acknowledgements, device protection requirements, and manager confirmation for approved arrangements. It should not pretend the organization can inspect every home office continuously.

Provider facility assurance should be used only for provider-controlled locations. NorthStar's office evidence does not protect Harbor Point's printed engineering documents; the cloud provider's data-center controls do not protect a customer laptop.

Lost keys and badges create useful test cases because they demonstrate revocation and replacement rather than merely issuance.

Evidence structure

Evidence layer	Typical content
Authorization	Access list
Entry	Badge/key records
Visitors	Log/escort
Restricted areas	Server room controls
Alternate sites	Remote-work requirements
Provider	Facility assurance

Frequent readiness failures

- Generic provider facility evidence used for customer office.
- Shared keys not attributable.
- Visitor log has no escort context.
- Remote work not included.
- Lost badge process never tested.

Evidence Playbook 11: Risk Assessment

Risk Assessment evidence should show both risk evaluation and vulnerability-management operation. The vulnerability side should begin with scope and coverage rather than severity counts.

Harbor Point reconciles the scanner target population to its in-scope asset inventory. Missing assets, failed credentials, unauthenticated scans, and excluded applications are tracked as coverage issues before the team reviews remediation metrics.

A strong vulnerability evidence chain follows a finding from discovery through ownership, remediation, exception if needed, and rescan. The package should preserve the before and after state so closure is demonstrable.

Risk assessment evidence should also show management evaluation beyond scanner output. Changes in architecture, threat environment, suppliers, and business operations may create risks that are not represented as CVEs.

Provider-scanning evidence should distinguish the service boundary. If NorthStar scans the customer environment but Harbor Point owns remediation scheduling, the evidence package should show the handoff and decision records.

Evidence structure

Evidence layer	Typical content
Risk review	Periodic risk assessment
Coverage	Scanner targets vs inventory
Findings	Representative vulnerabilities
Decision	Remediate/exception
Validation	Rescan

Frequent readiness failures

- Coverage percentage hides missing assets.
- Unauthenticated scans accepted as complete.
- No application vulnerability process.
- Tickets close before rescan.
- Risk register disconnected from technical changes.

Evidence Playbook 12: Security Assessment

Security Assessment evidence should demonstrate the customer’s own process for evaluating controls, tracking correction, monitoring performance, and maintaining the SSP. The outputs of Chapters 7 and 8 are evidence only if they are controlled, current, and connected to ongoing governance.

Harbor Point retains internal assessment findings with source evidence and reviewer notes. Remediation records link each finding to ownership, implementation change, validation, and closure. Closed items remain traceable rather than disappearing from the register.

Continuous monitoring evidence should be chosen based on the control. Access reviews, source-health reviews, vulnerability scans, backup tests, and provider reviews may all be monitoring activities when they are planned, performed, and acted upon.

SSP revision history should show that material changes and remediation outcomes update the documented system. An SSP that describes retired tools undermines the credibility of otherwise strong evidence.

Management review evidence shows that unresolved gaps, exceptions, and significant changes reach people with authority to allocate resources and accept decisions.

Evidence structure

Evidence layer	Typical content
Assessment	Internal review
Remediation	Action register
Closure	Re-test evidence
Monitoring	Recurring control checks
Documentation	SSP revision
Governance	Management review

Frequent readiness failures

- Findings disappear after closure.
- No re-test evidence.
- Monitoring reports created but not reviewed.
- SSP stale.
- Management not informed of material gaps.

Evidence Playbook 13: System and Communications Protection

This evidence package should make architecture and enforcement tell the same story. Network diagrams, data flows, firewall rules, cloud security groups, remote access, encryption, keys, certificates, and collaboration features must align.

Harbor Point starts with the current boundary and connection inventory. NorthStar then maps representative firewall and cloud rules to the documented connections. Unexplained rules are investigated rather than hidden.

Remote administrative paths are included separately because they may bypass user-facing network controls. RMM, vendor tunnels, site-to-site VPN, management interfaces, and cloud administration should be visible in the evidence architecture.

Encryption evidence should identify the actual protocol, configuration, or service feature in use. A vendor claim that traffic is encrypted is less persuasive than a tenant or system configuration that shows how Harbor Point uses the feature.

Certificate and key lifecycle records can demonstrate ownership, renewal, revocation, and controlled storage. The package should avoid exposing private keys or secrets.

Evidence structure

Evidence layer	Typical content
Architecture	Network/data-flow diagrams
Enforcement	Firewall/security groups
Remote paths	VPN/RMM/vendor
Encryption	Configured protocols/features
Keys/certs	Inventory and lifecycle

Frequent readiness failures

- Diagram and rules disagree.
- MSP remote channel missing from architecture.
- Provider claim used instead of tenant config.
- Certificate ownership unclear.
- Sensitive keys exposed in evidence.

Evidence Playbook 14: System and Information Integrity

Integrity evidence should show that flaws and malicious activity are detected, corrected, and verified across the complete in-scope asset population. Coverage reconciliation is the foundation.

NorthStar reconciles endpoint and server inventories against patching, EDR, antimalware, and advisory processes. Missing agents, stale check-ins, unsupported devices, and broad exclusions are tracked as explicit exceptions or gaps.

Patch evidence should show more than deployment success. For important corrections, the package can include update assignment, installation result, restart or state validation, and vulnerability rescan or version verification.

Advisory handling should connect external information to internal applicability. The organization should be able to show that relevant advisories are received, evaluated against asset inventory, and acted upon when applicable.

EDR exclusion evidence should be tightly controlled. Broad exclusions can undermine protection, so the package should preserve business reason, approval, scope, and periodic review.

Evidence structure

Evidence layer	Typical content
Coverage	Inventory vs protection
Patch	Deployment + validation
Malware	Agent health
Advisory	Receipt + applicability
Exception	Exclusions and compensating safeguards

Frequent readiness failures

- 99% coverage accepted without knowing missing 1%.
- Patch deployment marked success before verification.
- Broad EDR exclusions.
- Advisories not mapped to assets.
- Unsupported systems have no documented treatment.

Assessment Readiness Operations

Operations Practice 1: Evidence freeze without operational freeze

An evidence package may need a defined cut-off date for organization and review, but the production environment continues to change. Harbor Point records the assessment preparation date and then logs material changes that occur afterward. The team does not freeze security changes merely to preserve screenshots. Instead, it updates affected evidence and explains the change.

Management question: who owns this activity, what is the failure condition, and what record shows completion? Treating assessment logistics as an operating process reduces confusion and protects the production environment during high-pressure review periods.

Operations Practice 2: Assessment request intake

All requests are logged with requestor, objective or topic, owner, due date, status, and delivered artifact. The coordinator checks whether the request can be answered from the existing package or requires fresh source evidence. This prevents duplicate exports and conflicting versions.

Operations Practice 3: Interview scheduling

Interview schedules should group related topics where practical and provide backup personnel. The schedule should account for provider representatives, time zones, operational duties, and the possibility that a technician may be handling a live incident when originally scheduled.

Operations Practice 4: Demonstration safety

Demonstrations should use read-only access or controlled test accounts when practical. Any action that could alter production state should follow normal change control. The desire to demonstrate a control does not justify creating risk or bypassing procedure.

Operations Practice 5: Evidence delivery tracking

When evidence is delivered outside the internal repository, Harbor Point records what was sent, to whom, when, through which approved method, and whether the copy must later be removed. Sensitive technical material should not accumulate in uncontrolled email threads.

Operations Practice 6: Follow-up management

The coordinator maintains a question log that distinguishes open factual questions from potential findings. Teams should avoid premature debate. First establish the facts, then determine whether the implementation satisfies the requirement and objective.

Operations Practice 7: Provider escalation

Provider-dependent evidence requests should have an escalation path. Account management, contract owners, and service managers should know how to obtain higher-level support when ordinary support channels cannot produce the needed record.

Operations Practice 8: Assessment-period change management

Material changes during assessment activity should be reviewed for scope, implementation, evidence, and communication impact. A migration or emergency change may be necessary, but the organization should understand which prior evidence became stale and which new records must be produced.

Operations Practice 9: Sensitive-screen sharing

When demonstrating multi-tenant or sensitive consoles, use customer-scoped views, role-based access, or preapproved redaction where appropriate. The demonstrator should know which panes or records contain other-customer data or secrets and avoid exposing them inadvertently.

Operations Practice 10: Evidence closeout

After assessment or readiness review, temporary workspaces and duplicated files are reconciled. Required records are retained in controlled locations, unnecessary copies are removed, provider temporary access is revoked, and open findings transition into the remediation process.

Worked Evidence Scenarios

Scenario 1: The missing quarter

A quarterly privileged-access review exists for Q1 and Q3 but not Q2. Do not create a backdated review and pretend it occurred. Record the missing evidence, determine whether the review was actually omitted or merely not retained, evaluate the implementation impact, and correct the recurring process.

Evidence lesson: state what the current record proves, what is missing, and what process must change so the same weakness does not recur. Avoid manufacturing evidence after the fact. Correct the control and improve the record-generation process going forward.

Scenario 2: The perfect screenshot

A screenshot shows MFA enabled today, but the claim concerns sustained coverage for privileged users. Add population evidence, policy assignment, authentication records, exception history, and review evidence appropriate to the period.

Scenario 3: The provider report expires

Beacon's portal retains customer reports for only 90 days. If Harbor Point needs longer history, define a scheduled export or different service arrangement before older evidence disappears.

Scenario 4: The shared dashboard

NorthStar's RMM dashboard includes several customers. Use customer-scoped export or filtered view. Do not redact dozens of unrelated rows manually if the platform can generate a clean customer report.

Scenario 5: The stale SSP

The evidence package points to a retired VPN product. Update the SSP and related diagrams after verifying the current implementation. Preserve historical context if needed for the reviewed period.

Scenario 6: The closed vulnerability

A remediation ticket says complete, but the scanner still detects the issue. Keep the item open, investigate why the correction failed, and retain the successful rescan as closure evidence.

Scenario 7: The incident without a decision

SOC records show suspicious activity, but no record indicates whether Harbor Point declared an incident. Determine the actual decision, improve the workflow, and ensure future cases preserve decision authority.

Scenario 8: The missing technician

The only engineer who knows how to export a firewall rule report is on leave. Treat this as a retrieval-process weakness. Document the method and ensure a backup custodian can perform it.

Scenario 9: The changed cloud tier

A cloud service was upgraded and the provider assurance package changed. Revalidate the exact offering, region, responsibility matrix, tenant configuration, and evidence source.

Scenario 10: The evidence folder full of secrets

The readiness folder contains passwords and private keys pasted into screenshots. Remove unnecessary secrets, rotate exposed credentials if appropriate, and redesign evidence capture so controls can be demonstrated without revealing protected values.

Scenario 11: The clean policy, messy reality

Policy states all support sessions are approved, but tickets reveal technicians sometimes connect before approval in emergencies. Investigate the real emergency process, correct the implementation and policy, and preserve evidence of the approved emergency pathway.

Scenario 12: The transfer that kept old access

An employee changed departments. The new role was added, but the old project role remains. Correct the access, identify why the transfer workflow failed, and add lifecycle evidence to the personnel and access packages.

Scenario 13: The archive nobody can read

Logs were exported to long-term storage, but only the engineer who designed the archive understands the format. Improve retrieval, documentation, and backup custodian capability; retention without practical retrieval is weak readiness.

Scenario 14: The provider attestation with no scope

A letter says NorthStar follows strong security practices but does not identify the Harbor Point service. Replace or supplement it with service-specific evidence tied to the relevant responsibility.

Scenario 15: The assessment workspace that became permanent

Temporary assessment files remain in a collaboration folder months later. Reconcile them with retention, remove unnecessary copies, and preserve only controlled records that still have a defined purpose.

Review Questions

1. What is the difference between operational evidence and assessment-preparation evidence?

2. Why should an evidence index begin with assessment objectives rather than filenames?

3. What qualities should be evaluated before accepting an artifact as useful evidence?

4. Why is a current screenshot often insufficient for a recurring control?

5. How do population evidence and sample evidence complement one another?

6. What is the difference between source evidence and presentation evidence?

7. Why should authoritative repositories be distinguished from assessment copies?

8. What does an evidence custodian do?

9. Why should retention be determined by record type and governing source?

10. How can evidence notes improve continuity without replacing the source record?

11. Why should evidence retrieval be tested before assessment activity?

12. How should MSPs protect other customers when producing evidence from multi-tenant platforms?

13. What conditions should be checked before relying on provider assurance?

14. How should cloud evidence reflect shared responsibility?

15. Why can Security Protection Data make an evidence repository sensitive?

16. When is a provider attestation useful, and what should it contain?

17. Why should provider offboarding include evidence portability?

18. How should interviewees be prepared without coaching them to memorize answers?

19. What makes a technical demonstration effective and safe?

20. What should an assessment-day evidence workspace contain?

21. How should contradictory evidence be handled?

22. Why does an organized evidence package not guarantee an assessment result?

23. What evidence pattern best supports remediation closure?

24. How should evidence readiness be sustained through material changes?

Answer Guidance

Questions 1 through 6 focus on evidence quality and structure. Strong evidence comes from the normal operation of the control, is tied to the correct population and time period, and is selected according to the fact the assessment objective requires. Summaries help explanation but should not replace authoritative source records.

Questions 7 through 12 focus on repositories, custody, retention, and MSP delivery. The evidence program should preserve authoritative sources, identify responsible custodians, protect sensitive records, and ensure customer-specific attribution in multi-tenant systems.

Questions 13 through 17 focus on provider and cloud dependencies. Provider assurance must apply to the exact service and conditions used. Shared responsibility requires both provider evidence and customer-side implementation evidence. Offboarding should preserve the records the customer is authorized and required to retain.

Questions 18 through 24 focus on assessment readiness and sustainment. Personnel should understand real workflows, demonstrations should answer defined questions, contradictions should be investigated, and evidence sources should be updated through change management. Readiness supports an assessment but does not predetermine its outcome.

Key Terms

Term	Meaning in this chapter
Authoritative evidence source	The primary system, record, or controlled source relied upon for a fact.
Evidence index	A structured map connecting objectives, sources, custodians, scope, period, and retrieval.
Operational record	A record created because a security activity or system process occurred.
Presentation evidence	A summary or view created to help explain authoritative source evidence.
Population evidence	Evidence describing the complete relevant set of users, assets, events, or records.
Sample evidence	Selected examples used to examine the operation of a process in depth.
Evidence custodian	Role responsible for preserving, protecting, indexing, and retrieving evidence.

Evidence note	Short factual context explaining the source, scope, period, and relevance of an artifact.
Retrieval test	Exercise that verifies an authorized custodian can obtain and explain the expected record.
Assessment workspace	Controlled temporary location used to organize approved assessment materials.
Provider assurance	Provider-supplied evidence or attestation supporting a provider-performed responsibility.
Evidence portability	Ability to retain or transfer needed records when a service or provider changes.
Contradiction log	Record of material disagreements among artifacts or explanations that require resolution.
Evidence refresh trigger	Scheduled or event-based condition that causes evidence or its index entry to be updated.

Closing Perspective

CMMC evidence readiness is strongest when it is almost invisible to daily operations. The organization performs the right security work, the work naturally produces reliable records, and those records are protected and indexed so they can be retrieved when needed. The assessment package then becomes a view into normal operations rather than a separate compliance world.

For the MSP, this creates a clear service standard. Customer-specific evidence should be attributable, retrievable, protected, and tied to the exact service the MSP performs. Provider limitations should be known before they become assessment problems. Evidence delivery should be designed into contracts, platforms, retention, and technician workflows.

Harbor Point’s sequence now forms a coherent readiness system: identify information, define scope, assign responsibility, assess gaps, remediate weaknesses, and organize evidence of sustained implementation. The next stage is assessment execution itself—coordinating people, evidence, demonstrations, findings, and operational stability while the assessment is underway.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. Use the current provisions for scoping, assessment, external service providers, POA&M, affirmation, and assessment-artifact requirements.

R2. National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

R3. National Institute of Standards and Technology. NIST SP 800-171A, June 2018, Assessing Security Requirements for Controlled Unclassified Information. Used here for the applicable Revision 2 assessment objectives and examine, interview, and test methods.

R4. Office of Industrial Base Growth, July 13, 2026. Forging the Arsenal of Freedom: Department Suspends CMMC Phase II Requirements. The announcement states that Phase II implementation was suspended while Phase I self-assessment requirements remain in place and underlying safeguarding obligations continue.

R5. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Review the current clause and the customer’s actual contract for safeguarding, incident, preservation, cloud, and flow-down obligations.

R6. Current Department CMMC resources, FAQs, and acquisition guidance. Confirm current program status before relying on transition dates, assessment pathways, or implementation milestones.

Sources reviewed September 20, 2026. This chapter provides operational and educational guidance for evidence readiness. It does not replace the governing regulation, the applicable contract, legal advice, or an authorized CMMC assessment.

CMMC for MSPs

From Readiness to Certification

Chapter 10

Managing the CMMC Assessment Lifecycle

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and source context

10.1–10.8 Understanding the Level 2 certification assessment lifecycle

10.9–10.17 Pre-assessment governance, contracting, scope validation, and readiness gates

10.18–10.27 Assessment execution: examine, interview, test, evidence handling, and daily management

10.28–10.35 Findings, scoring, conditional status, POA&M closeout, reporting, and certification

10.36–10.43 MSP operating roles, communications, change control, and post-assessment sustainment

10.44–10.49 Harbor Point lifecycle case study, management dashboard, common failures, and chapter review

Key terms and official references

Chapter Purpose

Chapter 9 focused on building an evidence package that can withstand examination. Chapter 10 moves from readiness into the actual CMMC assessment lifecycle. The central problem is no longer simply whether the organization has evidence. The organization must now manage people, scope, systems, providers, logistics, decisions, findings, and deadlines while a C3PAO assessment team independently evaluates the implementation of Level 2 security requirements.

For an MSP, the assessment lifecycle creates a dual responsibility. The MSP may be part of the customer's security implementation and therefore an important source of evidence, demonstrations, technical explanations, and operational records. At the same time, the MSP must not interfere with assessor independence, coach customer personnel into artificial answers, hide weaknesses, or allow the assessment to become a performance staged for the assessment week. The provider's job is to make the real environment understandable and supportable.

This chapter treats the assessment as a managed lifecycle rather than a short event. It begins before the contract with a C3PAO is signed, continues through pre-assessment planning, evidence review, interviews and technical tests, findings and scoring, conditional status and POA&M closeout when permitted, certificate issuance, annual affirmation, and the three-year certification cycle. The emphasis is practical: what the

OSC and its MSP should do, who should own each action, what can go wrong, and how to preserve the integrity of the assessment.

Learning Objectives

- Explain the four phases of the CMMC Assessment Process for a Level 2 certification assessment.
- Distinguish the responsibilities of the Organization Seeking Certification, C3PAO, Lead CCA, assessment team, affirming official, and external service providers.
- Prepare assessment governance, communications, facilities, remote-access, evidence, and personnel before assessment activities begin.
- Validate the assessment scope against the systems, people, facilities, security protection assets, specialized assets, and service providers actually supporting the CUI environment.
- Coordinate examine, interview, and test activities without scripting or improperly influencing participants.
- Manage evidence requests and technical demonstrations in a controlled, traceable manner.
- Understand assessment scoring, MET and NOT MET determinations, conditional status, POA&M restrictions, and closeout responsibilities.
- Preserve assessment records and lessons learned while protecting CUI, customer data, and assessor-provided materials.
- Maintain certification readiness through annual affirmation, continuous change review, and preparation for the next assessment cycle.

Source and Applicability Note

This chapter is written for the CMMC Level 2 certification-assessment context and uses the CMMC program rule in 32 CFR Part 170, the Level 2 requirement baseline incorporated from NIST SP 800-171 Revision 2, NIST SP 800-171A assessment procedures, and the current CMMC Assessment Process (CAP) published by The Cyber AB. The CAP organizes a Level 2 certification assessment into four phases: Conduct the Pre-Assessment; Assess Conformity to Security Requirements; Complete and Report Assessment Results; and Issue Certificate and Closeout POA&M.

The exact contract requirement, assessment type, transition timing, and applicable CMMC status must be confirmed for the specific solicitation or contract. As of

September 2026, organizations should also verify current DoD implementation notices, DFARS requirements, and Cyber AB process updates before scheduling or conducting an assessment. This chapter therefore emphasizes durable assessment-management principles while identifying formal sources that should be checked for current procedural details.

The examples use the fictional company Harbor Point Engineering (HPE), its MSP NorthStar Managed Services, its MSSP Beacon Security Operations, and several cloud providers. The examples are intentionally written from the perspective of an OSC that relies materially on external providers while retaining accountability for its own CMMC status.

Current implementation context (September 2026). On July 13, 2026, the Department announced the immediate suspension of CMMC Phase II requirements that had been scheduled for November 10, 2026 while a reform review proceeds. Phase I self-assessment requirements and underlying contractual cybersecurity obligations remain relevant. This chapter therefore separates the durable mechanics of Level 2 certification-assessment management from acquisition timing. Organizations should verify the current DoD implementation notice, applicable solicitation or contract language, 32 CFR Part 170, and the current Cyber AB CMMC Assessment Process before scheduling or relying on a certification assessment milestone.

10.1 The Assessment Is a Lifecycle, Not an Audit Week

A CMMC Level 2 certification assessment is often described as a multi-day assessment event, but operationally it is a lifecycle that begins much earlier. The OSC selects a C3PAO, validates scope, prepares the assessment boundary, identifies responsible personnel, establishes secure ways to exchange information, and confirms that the environment presented to the assessor is the environment that actually processes, stores, or transmits CUI. After the assessment event, reporting, quality review, possible conditional-status closeout, certificate activities, annual affirmations, and continuous compliance remain.

Organizations that treat the assessment as a calendar appointment tend to discover problems too late. A system owner may be unavailable. A provider may require weeks to produce a customer-specific export. A remote demonstration may fail because the assessor cannot observe the relevant interface. A network segment may have changed since the SSP was updated. These are lifecycle-management failures rather than isolated technical failures.

Harbor Point therefore manages CMMC assessment readiness as a standing program. The same workstream that tracks remediation also tracks assessment dependencies,

key contacts, evidence owners, changes that affect scope, and upcoming affirmation or certification dates.

In practice, this is one of the areas where otherwise mature organizations can lose control of continuity across planning, assessment, reporting, and sustainment. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of the assessment is a lifecycle, not an audit week is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to treat assessment dependencies as a standing service-management workstream rather than a one-week project. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include a lifecycle calendar, dependency register, named owners, and recurring readiness reviews. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.2 Understand the Four CAP Phases

The current CMMC Assessment Process identifies four phases for Level 2 certification assessments. Phase 1 is Conduct the Pre-Assessment. Phase 2 is Assess Conformity to Security Requirements. Phase 3 is Complete and Report Assessment Results. Phase 4 is Issue Certificate and Closeout POA&M. The names matter because they separate preparation, evidence-based conformity decisions, formal reporting, and certification or conditional-status closure.

An OSC should not attempt to compress all four phases into one internal checklist. Each phase has different participants, decision rights, records, and risks. Scope questions dominate early. Evidence and demonstrations dominate Phase 2. Quality assurance and report accuracy dominate Phase 3. Certificate issuance, POA&M closure where permitted, and lifecycle transition dominate Phase 4.

NorthStar maps its customer-support tasks to the same four phases. That alignment prevents the MSP from continuing readiness-consulting behavior after the formal assessment has started in ways that could create confusion about assessor independence.

The operational significance of this section is easy to underestimate. It influences the handoff between the four CAP phases and the different decisions made in each phase. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of understand the four cap phases is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to map provider tasks to the phase in which they are appropriate so readiness consulting does not blur into assessment activity. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify

facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include phase-specific checklists, responsibility assignments, entry criteria, and closeout records. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.3 Preserve Assessor Independence

The C3PAO and its assessment team must make independent conformity determinations. The OSC and its MSP can provide evidence, answer questions, explain architecture, demonstrate systems, and correct factual misunderstandings. They should not pressure assessors to accept weak evidence, negotiate technical conclusions through sales channels, or instruct employees to give memorized answers that do not reflect actual practice.

Independence is especially important when the MSP previously helped the OSC prepare. The provider may know which evidence is strongest and which implementation areas were difficult. During the assessment, the provider should shift from advocate to factual participant. It responds to what is asked, identifies the authoritative source, explains service boundaries, and distinguishes facts from interpretation.

A useful internal rule is that preparation can improve the control and improve the evidence, but it should not manufacture a temporary version of reality. If the system would return to a weaker state after the assessors leave, the organization is not demonstrating sustainable implementation.

A strong CMMC program treats this as a management discipline because it shapes the credibility of an independent conformity determination. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of preserve assessor independence is therefore not administrative neatness. It is to keep the assessment anchored to the same environment,

responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore shift the MSP from readiness advocate to factual technical participant once formal assessment activity begins. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include conflict checks, role guidance, factual demonstrations, and a record of requested rather than volunteered evidence. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.4 Establish Assessment Governance

Harbor Point establishes a small assessment governance team before formal pre-assessment activities begin. The team includes an executive sponsor, assessment manager, CMMC program lead, technical lead, evidence coordinator, security lead, facilities contact, legal or contracts contact when needed, and named provider coordinators. Each role has authority boundaries and escalation paths.

The assessment manager controls the calendar, communications, participant scheduling, evidence-request workflow, and daily issue log. The technical lead coordinates demonstrations but does not answer governance questions on behalf of

policy owners. The evidence coordinator maintains the authoritative request tracker and prevents uncontrolled email attachments from becoming the de facto evidence repository.

Provider participation is planned rather than improvised. NorthStar identifies one primary and one backup contact. Beacon does the same for SOC-related questions. Cloud-provider evidence that cannot be generated live is collected and indexed in advance.

This topic deserves more attention than a checklist item because it directly affects clear authority, accountability, and escalation during a time-sensitive event. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of establish assessment governance is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to establish an assessment manager, evidence coordinator, technical lead, executive sponsor, and provider coordinators with explicit boundaries. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include a governance roster, escalation matrix, communications plan, and decision log. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team

has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.5 Define Decision Rights Before Pressure Arrives

Assessments create time pressure. Without predefined decision rights, every question can become an executive escalation. Harbor Point defines who can approve additional evidence release, who can authorize remote technical access, who can extend assessment-day hours, who can speak for contractual matters, and who can confirm that a factual correction should be submitted to the assessment team.

Decision rights should not be confused with answer ownership. A senior executive may authorize disclosure of a sensitive architecture diagram, but the network engineer remains the person best positioned to explain the diagram. Similarly, the MSP service manager may coordinate NorthStar personnel, while a platform engineer performs the actual demonstration.

Clear decision rights reduce delay and reduce the risk that participants make ad hoc concessions under pressure, such as sharing unnecessary multi-tenant data or granting broad assessor access to production systems.

In practice, this is one of the areas where otherwise mature organizations can lose control of avoiding improvised disclosures or operational decisions under pressure. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of define decision rights before pressure arrives is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to pre-authorize who may approve evidence release, remote access, schedule changes, sensitive demonstrations, and contractual clarifications. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall

within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include a decision-rights matrix tied to security, legal, technical, and executive approvals. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.6 Separate Assessment Management from Control Ownership

The person coordinating the assessment should not become the universal spokesperson for every security requirement. A mature implementation distributes knowledge across system owners, security personnel, administrators, HR, facilities, contracts, and providers. The assessment should reveal that operating model rather than conceal it.

Harbor Point uses the responsibility matrix developed earlier in the readiness program to identify the appropriate interviewee and demonstrator for each requirement family. The assessment manager knows where to route the question but does not replace the control owner.

This separation also improves credibility. When the individual who actually performs access reviews can explain the process, show the record, and discuss exceptions, the assessor can connect documentation to real operations.

The operational significance of this section is easy to underestimate. It influences preserving authentic control ownership and avoiding a single spokesperson who cannot prove daily operation. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of separate assessment management from control ownership is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this

discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to route questions to the people who actually perform, approve, monitor, or review the relevant activity. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include a control-owner map linked to interviewees, backups, systems, and evidence sources. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.7 Build a Single Assessment Calendar

The assessment calendar should integrate C3PAO milestones, internal readiness gates, provider dependencies, participant availability, facility access, change freezes where appropriate, backup dates, and post-assessment obligations. Harbor Point uses one controlled calendar rather than separate spreadsheets maintained by each team.

Key dates include scope-validation meetings, evidence-transfer windows, pre-assessment meetings, formal assessment dates, scheduled interviews, technical demonstrations, daily closeouts, anticipated report-review milestones, conditional-status deadlines when applicable, and annual affirmation dates.

The calendar is not merely administrative. A major infrastructure migration scheduled two days before assessment creates a technical and evidentiary risk. The

calendar makes those conflicts visible early enough for leadership to make an informed decision.

A strong CMMC program treats this as a management discipline because it shapes making dependencies, conflicts, and deadlines visible before they become assessment-day failures. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of build a single assessment calendar is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore integrate provider lead times, staff availability, evidence windows, facility access, and change events into one controlled calendar. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include a master calendar with milestones, owners, dependencies, contingency dates, and post-assessment obligations. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.8 Use Readiness Gates Instead of Optimism

Harbor Point does not declare itself ready because most remediation tasks are green. It uses readiness gates. A gate has objective exit criteria such as validated scope, approved SSP, reconciled asset inventory, tested evidence retrieval, completed interview preparation, resolved critical provider gaps, and successful demonstrations for representative technical requirements.

A failed gate does not automatically mean the assessment must be canceled, but it forces an explicit risk decision. Leadership sees what is incomplete, why it matters, and what consequence could follow during the assessment.

Readiness gates also protect the MSP. NorthStar can state precisely which customer dependencies remain open instead of being asked to provide a vague guarantee that the customer is ready.

A readiness decision should be based on verified exit criteria, not confidence, schedule pressure, or the percentage of tasks marked complete.

This topic deserves more attention than a checklist item because it directly affects replacing optimism with objective evidence that the organization can sustain what it claims. During lifecycle governance and readiness, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of use readiness gates instead of optimism is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to use gates for scope, SSP accuracy, evidence retrieval, provider readiness, interview readiness, and demonstrations. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from

assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include signed gate criteria, exception decisions, unresolved-risk summaries, and retest results. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

Assessment Governance Field Guide

Role	Primary responsibility	Do not substitute for
Executive sponsor	Risk decisions, resources, escalation	Technical demonstrator
Assessment manager	Calendar, coordination, issue flow	Control owner
Evidence coordinator	Request tracking and controlled release	Assessor
Technical lead	Technical sessions and safe demonstrations	Policy owner
Provider coordinator	MSP/MSSP participation and dependencies	Customer accountable official

10.9 Select a C3PAO Through Due Diligence

Choosing a C3PAO is not the same as shopping only on price or earliest available date. The OSC should confirm that the organization appears in the official Cyber AB ecosystem, understand the proposed assessment approach, clarify scheduling assumptions, review contractual terms, and confirm how sensitive evidence will be exchanged and protected.

Due diligence can include the C3PAO’s experience with organizations of similar complexity, ability to support required locations or remote activities, proposed assessment-team composition, conflict-of-interest controls, quality-assurance process, evidence-transfer approach, change and cancellation terms, and process for handling factual questions or appeals.

The OSC should not select a C3PAO because it promises an easy assessment or guaranteed result. A credible assessment provider should emphasize independence, evidence, process, and transparent expectations rather than certainty about an outcome before the assessment occurs.

In practice, this is one of the areas where otherwise mature organizations can lose control of selecting an assessment partner on competence, independence, process maturity, and fit rather than promises. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of select a c3pao through due diligence is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to evaluate C3PAO experience with comparable environments and external-service-provider complexity without seeking a guaranteed outcome. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include marketplace verification, conflict review, proposal comparison, references, and documented selection rationale. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve

the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.10 Review the Assessment Contract Carefully

The assessment contract should be read as an operational document. Harbor Point reviews scope assumptions, locations, estimated duration, participant expectations, travel terms, remote-assessment provisions, evidence-handling requirements, confidentiality, intellectual-property terms, report deliverables, payment milestones, cancellation or rescheduling, and the process for changes.

The contract should also identify what happens when the assessment scope differs materially from what was proposed. A newly identified enclave or additional facility can change assessment effort. The OSC should understand who authorizes that change and how it affects schedule and cost.

NorthStar reviews the portions that affect its participation but does not become the contracting party unless that arrangement is deliberate. Harbor Point retains visibility into the agreement governing its certification assessment.

The operational significance of this section is easy to underestimate. It influences turning the assessment agreement into an executable operating plan. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of review the assessment contract carefully is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to review the contract for scope assumptions, evidence handling, remote work, travel, changes, cancellations, confidentiality, and provider participation. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being

expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include a contract review checklist, resolved assumptions, named contacts, and approved change-control path. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.11 Validate Scope Again Before the Assessment

Scope validation is repeated because environments change. The assessment scope should reflect the current systems and organizational components that process, store, or transmit CUI, as well as assets and services that provide security protection or otherwise fall into applicable CMMC scoping categories.

Harbor Point reconciles the SSP boundary with network diagrams, asset inventory, identity systems, cloud tenants, backup services, security tools, remote-access methods, facilities, specialized assets, and provider dependencies. Any discrepancy becomes a tracked scope question rather than an assumption.

NorthStar performs its own customer-tenant reconciliation. It verifies which RMM tenant, security profiles, backup policies, identity groups, and support workflows correspond to Harbor Point. This reduces the chance that a demonstration accidentally uses another customer or an out-of-scope management path.

A strong CMMC program treats this as a management discipline because it shapes preventing certification decisions from being based on a stale or incomplete boundary. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of validate scope again before the assessment is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of

evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore reconcile the OSC boundary to MSP tools, cloud tenants, identity, backup, logging, remote access, facilities, and specialized assets. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include a scope reconciliation package with diagrams, inventories, service mappings, and tracked discrepancies. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.12 Confirm Every Assessment Location

Locations can include headquarters, satellite offices, data centers, manufacturing areas, remote-worker arrangements, provider facilities when relevant to the service relationship, and virtual or cloud environments. The assessment team needs a practical understanding of where in-scope activity occurs and how it will be observed.

Physical-access logistics should be planned early. Harbor Point identifies visitor procedures, escort rules, photography restrictions, secure meeting rooms, badge requirements, equipment restrictions, and areas where CUI may be present. If assessors need to observe a server room or controlled area, the visit should be feasible without improvisation.

Remote locations need equal attention. A remote employee using a company-managed endpoint may demonstrate controls through a video session, but the organization still must explain the operating environment, connectivity, physical expectations, and technical protections.

This topic deserves more attention than a checklist item because it directly affects ensuring the assessment can observe where in-scope work actually occurs. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of confirm every assessment location is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to plan physical and remote logistics for headquarters, satellite sites, remote workers, cloud environments, and provider-supported functions. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include location inventories, access procedures, remote-session plans, visitor controls, and location-to-scope mappings. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.13 Reconcile the SSP to the Environment

The SSP is a central narrative of the system and the implementation of requirements. Before formal assessment, Harbor Point conducts a final reconciliation between SSP statements and observable reality. It checks system names, provider names, technologies, network zones, responsible roles, procedures, and implementation descriptions.

This is not a cosmetic proofreading exercise. If the SSP says NorthStar performs quarterly privileged-access reviews but Harbor Point actually performs the review while NorthStar only exports data, the document misstates responsibility. If the SSP references a retired VPN, the assessment narrative is stale.

Any late correction should be controlled and explainable. The goal is an accurate SSP, not a document that changes repeatedly in response to anticipated assessor preferences.

In practice, this is one of the areas where otherwise mature organizations can lose control of keeping the SSP as an accurate description of the real system rather than an aspirational narrative. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of reconcile the ssp to the environment is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to compare responsibilities, technologies, diagrams, workflows, and service-provider statements against current operations. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include a final SSP reconciliation record with controlled corrections and approver signoff. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.14 Freeze the Evidence Index, Not the Environment

Organizations sometimes discuss a change freeze before assessment. A complete operational freeze is rarely practical and can create new risk. Harbor Point instead freezes the baseline evidence index and assessment package at a known point while continuing normal operations under controlled change management.

If a legitimate change occurs after the baseline is established, the evidence coordinator records the change, affected controls, updated artifacts, and whether the assessment team needs to be informed. This preserves traceability without pretending the environment stopped evolving.

Emergency security changes should never be delayed simply to preserve an assessment screenshot. Security comes first. The lifecycle process must be able to absorb and explain legitimate changes.

The operational significance of this section is easy to underestimate. It influences maintaining traceability while normal operations and legitimate security changes continue. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of freeze the evidence index, not the environment is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to baseline the evidence package and index while routing

subsequent changes through normal change management. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include a dated baseline, change log, replacement artifacts, affected-control analysis, and assessor notification decisions. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.15 Conduct a Formal Readiness Review

A readiness review is a management decision point. Harbor Point presents status by scope, control implementation, evidence readiness, provider dependency, interview readiness, technical demonstration readiness, documentation accuracy, and unresolved risks.

The review distinguishes three categories: ready and verified; ready with a documented operational risk; and not ready. Items in the third category require a decision to remediate, reschedule, or proceed with known exposure. The decision and rationale are recorded.

This discipline prevents last-minute optimism from overriding months of evidence. It also gives executives a defensible understanding of what the assessment team is likely to encounter.

A strong CMMC program treats this as a management discipline because it shapes creating a management decision point before formal assessment exposure. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency

was never assigned. The purpose of conduct a formal readiness review is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore present scope, evidence, personnel, provider, technical, documentation, and unresolved-risk status to leadership. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include a readiness review packet, red/amber/green criteria, exception approvals, and proceed/reschedule rationale. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.16 Prepare the Assessment Team Roster

Harbor Point builds a roster that maps each expected subject area to a primary participant and backup. It includes contact information, role, location, availability, control areas, and provider affiliation. Backups matter because illness, travel, incidents, or customer emergencies can occur during the assessment.

Participants receive logistical information and a concise explanation of the assessment process. They are told to answer factual questions directly, ask for

clarification when they do not understand the question, avoid speculation, and retrieve supporting records through the controlled evidence process.

Executives are prepared for governance questions without being trained to recite technical implementation details. Technical staff are prepared to demonstrate systems without being asked to speak for contractual or enterprise-risk decisions outside their role.

This topic deserves more attention than a checklist item because it directly affects ensuring the correct person is available for every governance, process, and technical topic. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of prepare the assessment team roster is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to build primary and backup coverage across customer personnel, MSP engineering, MSSP operations, HR, facilities, legal, and executives. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include a roster mapped to topics, time zones, availability, contact methods, and backup coverage. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control

appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.17 Run Mock Interviews Without Scripting Answers

Mock interviews are useful when they teach participants how to explain their real work. They become harmful when they provide memorized scripts. Harbor Point asks open questions such as how privileged access is requested, what happens when a user leaves, how failed backups are handled, or how incidents are escalated.

The facilitator listens for gaps between policy and practice. If an administrator says, “I usually just message the service desk,” while the procedure requires an approved ticket, the issue is investigated. The solution is to correct the process or documentation, not to tell the administrator what sentence to say during the assessment.

NorthStar uses the same rule with its technicians. They practice locating customer-specific evidence and explaining service boundaries, but they are expected to describe actual operations in their own words.

In practice, this is one of the areas where otherwise mature organizations can lose control of helping staff explain actual practice clearly without creating assessment theater. During pre-assessment planning and readiness validation, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of run mock interviews without scripting answers is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to use open-ended practice questions and correct process gaps rather than memorizing model answers. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary

and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include mock-interview notes, identified process/documentation gaps, participant guidance, and follow-up actions. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.18 Prepare Technical Demonstrations

Technical demonstrations should be rehearsed for reliability rather than theatrical effect. The team verifies required accounts, network connectivity, screen-sharing capability, test data, permissions, logging, and safe ways to demonstrate controls without exposing unrelated customer information or sensitive secrets.

Each demonstration has an owner and a fallback. For example, if Harbor Point must demonstrate multi-factor authentication, the identity engineer identifies a safe test account and the logs that show the event. If a live system is temporarily unavailable, the team knows which authoritative records can explain the outage and whether rescheduling is possible.

Demonstrations should use the production implementation or an appropriate representation of the actual control. A lab environment that is configured differently from production cannot substitute for the real implementation unless the assessment team explicitly accepts it for the question being examined.

The operational significance of this section is easy to underestimate. It influences showing real technical behavior safely and repeatably. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of prepare technical demonstrations is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of

evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to prepare test accounts, customer-scoped views, representative data, screen-sharing safeguards, and fallback evidence without staging a fake environment. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include demonstration runbooks, prerequisites, expected results, fallback artifacts, and test records. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.19 Create a Controlled Evidence-Request Workflow

During the assessment, new evidence requests are inevitable. Harbor Point uses one request tracker with a unique identifier, request text, requesting assessor, assigned owner, due time, status, artifact location, review state, and delivery confirmation.

The evidence coordinator performs a release check. The check confirms that the artifact answers the request, belongs to the correct customer and period, contains no unnecessary secrets or unrelated customer data, and has enough context to be understood. This is quality control, not censorship.

Email is used for notification rather than uncontrolled evidence storage whenever possible. Large or sensitive artifacts are exchanged through the agreed secure mechanism.

One request tracker, one evidence coordinator, and one approved transfer path reduce confusion and protect sensitive assessment material.

A strong CMMC program treats this as a management discipline because it shapes preventing ad hoc evidence sharing from creating confusion, leakage, and contradictory versions. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of create a controlled evidence-request workflow is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore route every new request through one tracker, one accountable owner, one review step, and an approved secure transfer path. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include unique request IDs, status, owner, due time, artifact link, release check, and delivery confirmation. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

Evidence Request Control Fields

Field	Purpose
Request ID	One traceable identifier across messages and repositories
Request text	Preserve exactly what was asked
Owner / provider	Identify who must produce or explain the artifact
Due time	Make assessment-day urgency visible
Release review	Confirm scope, relevance, secrets, and cross-customer exposure
Delivery record	Show what was sent, when, and through which approved channel

10.20 Begin Phase 2 with Shared Expectations

At the start of conformity assessment activities, the OSC should understand the schedule, communication channel, daily cadence, evidence-request process, and how interviews or demonstrations will be coordinated. Ambiguity early creates unnecessary friction later.

Harbor Point identifies one operational contact for the assessment team so assessors do not need to chase individual employees for logistics. At the same time, assessors retain direct access to appropriate interviewees and demonstrators. The coordinator manages access; it does not filter substantive answers.

NorthStar participates only when needed. Keeping every MSP engineer in every session wastes time and increases the risk of conflicting explanations.

This topic deserves more attention than a checklist item because it directly affects establishing a predictable operating rhythm when formal conformity assessment begins. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of begin phase 2 with shared expectations is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to agree on logistics, contact points, request handling, daily cadence, and provider participation without filtering substantive assessor access. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include kickoff notes, schedule, contact map, request protocol, and session plan. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.21 Understand Examine, Interview, and Test

NIST SP 800-171A and the CMMC assessment approach rely on assessment methods commonly described as examine, interview, and test. Examine reviews documentation and records. Interview gathers information from people who have knowledge of or responsibility for the control. Test exercises mechanisms or activities to verify behavior.

No single method should be treated as universally sufficient. A policy can show management intent but not prove configuration. A screenshot can show a setting but may not prove a recurring process. An interview can explain practice but may require corroborating records. A test can show technical behavior but may not explain governance or coverage.

Harbor Point prepares evidence packages so these methods reinforce one another. The SSP provides narrative, operational records show history, responsible personnel explain the process, and demonstrations verify important technical behavior.

In practice, this is one of the areas where otherwise mature organizations can lose control of understanding that policy, testimony, and technical behavior answer different kinds of assessment questions. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of understand examine, interview, and test is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to prepare complementary documentation, knowledgeable personnel, and safe demonstrations so examine, interview, and test reinforce one another. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include objective-to-method mapping and cross-referenced artifacts showing coverage across methods. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.22 Manage Interviews as Evidence-Producing Activities

An interview is not an oral exam in which a participant succeeds by remembering vocabulary. It is a way for the assessment team to understand how the organization performs the security requirement, who participates, what happens when exceptions occur, and where supporting records exist.

Participants should answer within their role. “I do not own that process, but the HR security coordinator does” can be a strong answer when accurate. Guessing creates contradictions that later require explanation.

The assessment coordinator records action items that arise from interviews, such as locating a referenced ticket or scheduling a specialist. The coordinator does not create a parallel transcript designed to challenge every assessor interpretation in real time.

The operational significance of this section is easy to underestimate. It influences using interviews to understand how work is really performed, including exceptions and handoffs. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of manage interviews as evidence-producing activities is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to coach personnel only on process awareness and evidence location, not on predetermined wording. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the

minimum evidence should include role-specific interview maps, process records, exception examples, and follow-up evidence requests. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.23 Manage Technical Tests Safely

Technical tests can touch identity, endpoint, network, logging, backup, vulnerability, encryption, and security-management systems. Testing must be coordinated so the assessment does not create operational instability or expose unnecessary information.

Harbor Point establishes boundaries for actions that could disrupt service. A demonstration of account lockout can use a test account. A backup restore can use designated data. A logging demonstration can generate a benign test event. Production-destructive actions are avoided unless specifically justified and safely controlled.

Provider platforms need additional safeguards. NorthStar uses customer-scoped views and test objects where possible. It does not grant broad administrative access to its entire multi-tenant RMM environment merely to make a demonstration convenient.

A strong CMMC program treats this as a management discipline because it shapes verifying controls without causing outages, destructive changes, or cross-customer exposure. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of manage technical tests safely is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore define safe test objects, customer-scoped views, maintenance constraints, rollback expectations, and escalation paths. This should be written into normal service

delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include test plans, approved boundaries, benign test events, captured results, and cleanup records. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.24 Keep an Assessment-Day Decision Log

The assessment manager maintains a concise decision log for material events: changed schedule, clarified scope, newly requested evidence, provider limitations, significant factual corrections, technical problems, and agreed follow-up actions. The log records facts and owners, not arguments.

This log becomes invaluable when several sessions occur in parallel. It prevents the morning team from assuming the afternoon team already delivered an artifact. It also helps Harbor Point distinguish an assessor request from an internal idea that emerged during a side conversation.

After the assessment, the log supports lessons learned and remediation without becoming a substitute for the official assessment report.

This topic deserves more attention than a checklist item because it directly affects preserving a reliable chronology of material decisions and unresolved actions. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of keep an assessment-day decision log is therefore not administrative neatness. It is to keep the assessment anchored to the same environment,

responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to record schedule changes, scope clarifications, evidence commitments, provider limitations, and factual corrections in one concise log. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include a timestamped decision log with owner, rationale, action, and closure status. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.25 Hold Daily Internal Closeouts

At the end of each assessment day, Harbor Point holds a short internal closeout. The team reviews completed sessions, open requests, upcoming interviews, technical issues, scope questions, and provider actions. The purpose is coordination, not an attempt to predict the score requirement by requirement.

Open evidence requests are assigned with due times. Contradictory statements are investigated. If a participant identified a genuine process weakness, the team records it as a potential remediation item rather than coaching the participant to revise the story.

The closeout also protects staff from fatigue. The assessment manager can decide which issues truly require evening work and which can wait for the next planned session.

In practice, this is one of the areas where otherwise mature organizations can lose control of preventing small issues from becoming next-day surprises while avoiding speculative scoring sessions. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of hold daily internal closeouts is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to hold short internal closeouts focused on completed work, open requests, contradictions, provider actions, and next-day readiness. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include daily closeout notes, action assignments, due times, and updated request/decision trackers. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.26 Communicate Factual Corrections Professionally

Assessments involve complex environments, so factual misunderstandings can occur. Harbor Point uses a disciplined correction method: identify the statement, provide the authoritative fact, show supporting evidence when appropriate, and avoid argumentative language.

For example, if an assessor believes a cloud backup repository is outside the defined boundary but the architecture shows it stores CUI, the team should clarify the architecture and scope implications immediately. If the disagreement concerns an assessment determination rather than a simple fact, the OSC follows the C3PAO's established process.

NorthStar avoids sales-style persuasion. Its role is to explain exactly what the service does, what the customer configures, what logs exist, and what limitations apply.

The operational significance of this section is easy to underestimate. It influences correcting misunderstandings without undermining professionalism or assessor independence. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of communicate factual corrections professionally is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to separate objective factual corrections from disagreement with an assessment judgment and use the established channel for each. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include a correction record identifying the fact, authoritative source, supporting evidence, and disposition. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.27 Protect Sensitive Information During Assessment

Assessment evidence can expose CUI, vulnerability details, security architecture, identity information, incident records, cryptographic settings, and provider administration. Harbor Point applies need-to-know, secure transfer, controlled storage, and clean-desk or secure-room practices throughout the assessment.

Screensharing deserves special attention. Participants close unrelated windows, disable unnecessary notifications, verify the correct tenant, and avoid exposing passwords, API keys, recovery codes, or unrelated customer data.

Physical notes, downloaded exports, and temporary files are handled under the same discipline. Assessment convenience is not a reason to create unmanaged copies of sensitive information.

A strong CMMC program treats this as a management discipline because it shapes protecting CUI, credentials, vulnerabilities, and multi-tenant provider data while demonstrating controls. During formal assessment execution, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of protect sensitive information during assessment is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore apply need-to-know, secure transfer, tenant filtering, screen hygiene, temporary-file controls, and cleanup throughout the event. This should be written into normal

service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include access logs, transfer records, workspace permissions, clean-up checklists, and data-handling instructions. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.28 Understand MET and NOT MET Determinations

At the requirement level, the assessment team makes conformity determinations based on the evidence obtained through the assessment methods. The OSC should focus on providing complete, relevant evidence rather than trying to negotiate terminology while the evidence is still incomplete.

A requirement that appears implemented in policy but cannot be demonstrated operationally may still present a problem. Likewise, a technical setting may exist on some assets but fail to cover the defined population. The determination depends on the implementation being assessed, not on the organization’s intentions.

Harbor Point therefore treats any questioned requirement as an evidence-and-implementation investigation: what exactly is implemented, where, for whom, by whom, since when, and what authoritative record demonstrates it.

This topic deserves more attention than a checklist item because it directly affects understanding that conformity is determined from implemented and adequately supported requirements, not intent. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may

discover that an important dependency was never assigned. The purpose of understand met and not met determinations is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to investigate questioned requirements by population, scope, owner, duration, configuration, and operational history rather than arguing labels. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include objective-level evidence showing what is implemented, where, for whom, by whom, and since when. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.29 Understand CMMC Scoring

CMMC Level 2 uses the scoring methodology tied to the 110 NIST SP 800-171 Revision 2 requirements and the DoD Assessment Methodology. Requirements do not all carry the same point value. Some unmet requirements have larger scoring consequences because of their security significance.

The readiness program should know the scoring implications before assessment, but scoring is not a substitute for compliance. An organization should not deliberately

leave a requirement weak because it believes the score impact is small. Contract requirements, POA&M restrictions, conditional-status rules, and security risk all matter.

NorthStar can help the customer understand which provider-supported requirements have high operational significance, but the C3PAO assessment team is responsible for the formal assessment determination and score.

In practice, this is one of the areas where otherwise mature organizations can lose control of understanding score consequences without reducing compliance to arithmetic. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of understand cmmc scoring is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to use scoring knowledge for risk awareness and remediation planning while continuing to treat every applicable requirement as a required security outcome. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include an internal score model tied to authoritative methodology, gap status, POA&M eligibility, and management risk context. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one

person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

Assessment Outcome Management View

Condition	Management response	Evidence focus
Requirement questioned	Clarify implementation and population	Authoritative configuration and operating records
NOT MET determination	Understand precise deficiency and consequence	Original finding context and objective-level evidence
Conditional pathway available	Launch executive-owned closure program	POA&M eligibility, milestones, and closeout proof
Final status achieved	Transition to sustainment	Lifecycle dates, affirmation, change monitoring

10.30 Distinguish Final and Conditional Level 2 Status

Under the CMMC program, Level 2 assessments can result in final or conditional status when regulatory conditions are met. Conditional status is not the same as ignoring deficiencies. It is a time-limited pathway governed by specific scoring thresholds, POA&M restrictions, and closeout requirements.

Harbor Point plans for final status and treats conditional status as an exception path. Before assessment it identifies requirements that cannot be placed on a POA&M and verifies that high-risk dependencies are fully implemented. The organization does not assume every gap can be fixed later.

If conditional status occurs, executive attention increases rather than decreases. The remaining work now has a formal deadline and direct certification consequence.

Conditional status is a governed, time-limited exception path—not a substitute for implementing the required security program.

The operational significance of this section is easy to underestimate. It influences distinguishing a completed certification outcome from a time-limited conditional pathway. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of distinguish final and conditional level 2 status is therefore not administrative neatness. It is to keep the assessment

anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to plan for final status and treat conditional status as an exception requiring immediate executive ownership and disciplined closure. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include status records, eligible POA&M items, deadlines, restrictions, owners, and closeout evidence plans. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.31 Manage a Conditional POA&M as a Program

When a permitted deficiency remains under conditional status, Harbor Point creates a closure workstream with accountable owner, technical tasks, evidence expectations, validation activities, provider dependencies, change-control needs, and a deadline aligned to the CMMC rules and C3PAO process.

The closure plan should start with root cause. If a requirement failed because endpoint coverage was incomplete, simply taking a new screenshot of the console does not prove the population is now complete. The team reconciles the inventory, deploys the control, verifies exceptions, and creates evidence that demonstrates sustainable correction.

NorthStar tracks customer POA&M closure separately from ordinary service tickets so urgency, evidence, and validation are visible to leadership.

A strong CMMC program treats this as a management discipline because it shapes preventing conditional status from becoming ordinary backlog management. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of manage a conditional poa&m as a program is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore create a dedicated closure program with root-cause correction, implementation, testing, evidence, executive visibility, and deadline protection. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include a conditional POA&M workstream with milestones, validation results, dependencies, and escalation triggers. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.32 Prepare for POA&M Closeout Assessment Activities

Closeout is an assessment activity, not an internal declaration. The OSC should know what evidence will demonstrate that each permitted deficiency has been corrected and be prepared for any required examine, interview, or test activities.

Harbor Point preserves the original finding context so the closeout evidence answers the actual weakness. A corrected policy alone is insufficient when the original issue was a technical enforcement failure. A technical change alone may be insufficient when the original issue included missing process governance.

The team tests retrieval and demonstrations before the closeout session exactly as it did before the main assessment.

This topic deserves more attention than a checklist item because it directly affects proving that a permitted deficiency has actually been corrected rather than merely documented. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of prepare for poa&m closeout assessment activities is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to recreate the original assessment context and prepare examine, interview, and test evidence that addresses the precise weakness. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include before/after evidence, corrected population,

retest results, updated documentation, and closeout-session readiness. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.33 Review Draft or Preliminary Results for Factual Accuracy

When the C3PAO provides an opportunity to review information, Harbor Point focuses on factual accuracy, completeness, scope identification, and correct representation of evidence. It distinguishes an objective factual error from disagreement with professional judgment.

Factual corrections are concise and supported. If the report lists the wrong cloud service, the team supplies the correct service information. If an assessment conclusion remains unfavorable after the facts are understood, the organization uses the applicable C3PAO or Cyber AB processes rather than editing its internal copy to tell a different story.

This disciplined approach preserves the official record and reduces confusion between internal readiness analysis and the formal assessment result.

In practice, this is one of the areas where otherwise mature organizations can lose control of keeping the official record accurate while respecting the distinction between facts and assessor judgment. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of review draft or preliminary results for factual accuracy is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to review names, scope, services, dates, evidence references, and factual descriptions carefully and submit concise supported corrections. This

should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include a controlled factual-accuracy review with source references and tracked responses. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.34 Understand Reporting and Quality Assurance

Phase 3 includes completing and reporting assessment results. The C3PAO’s internal quality process is important because the assessment must be consistent, supportable, and documented. The OSC should expect that the assessment team may need time after active assessment sessions to complete records and quality review.

Harbor Point keeps its assessment support team available for legitimate clarification requests during this period but does not continue sending unsolicited evidence in an attempt to reopen completed determinations unless the process permits it.

NorthStar preserves the evidence and demonstration records it provided so later questions can be answered consistently.

The operational significance of this section is easy to underestimate. It influences allowing the C3PAO to complete quality review without creating contradictory post-assessment evidence streams. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of understand reporting and quality assurance is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and

operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to keep knowledgeable contacts available for clarification but avoid unsolicited material unless the process permits it. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include clarification requests, preserved submitted evidence, report-review records, and internal communication controls. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.35 Move from Assessment Result to Certification Lifecycle

Phase 4 addresses certificate issuance and POA&M closeout. Once the applicable final Level 2 status is achieved and the required process is completed, the organization transitions from assessment-project mode back to continuous compliance management.

This transition should be formal. Harbor Point records certification identifiers and dates, updates the compliance calendar, preserves official records, closes temporary assessment access, inventories lessons learned, and assigns post-assessment improvements.

The moment after certification is a dangerous time for complacency. The environment will continue to change, and annual affirmation of continuous compliance remains an important lifecycle obligation.

A strong CMMC program treats this as a management discipline because it shapes turning a one-time result into a managed certification lifecycle. During findings, scoring, reporting, and closeout, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of move from assessment result to certification lifecycle is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore close temporary assessment mechanisms, record status and dates, preserve required records, capture lessons, and resume continuous control monitoring. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include certification records, lifecycle calendar, cleanup checklist, improvement backlog, and recurring compliance reviews. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.36 Manage Annual Affirmation of Continuous Compliance

CMMC is not designed as a three-year period of silence between assessments. The regulatory framework includes annual affirmation requirements. Harbor Point therefore maintains an annual affirmation readiness process that reviews material changes, unresolved control failures, scope changes, provider changes, and evidence supporting continued implementation.

The affirming official should receive a meaningful compliance picture rather than a ceremonial signature request. Management reviews current status, material exceptions, relevant incidents, significant architectural changes, and the results of internal validation.

NorthStar supplies customer-specific service and control information needed for that review, but Harbor Point remains responsible for its own affirmation.

This topic deserves more attention than a checklist item because it directly affects making annual affirmation a substantive management decision supported by current information. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of manage annual affirmation of continuous compliance is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to provide the affirming official with changes, exceptions, incidents, provider changes, scope updates, and validation results rather than a ceremonial signature request. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include an affirmation package, management review minutes, current scope, exceptions, and signed affirmation record. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.37 Treat Material Change as a Certification Risk Event

Mergers, acquisitions, office moves, cloud migrations, identity-platform replacements, new remote-access methods, MSP transitions, major network redesigns, and new CUI workflows can affect the basis on which the organization was assessed. Harbor Point uses a material-change review to determine whether scope, SSP content, controls, responsibilities, or evidence sources must be updated.

The review is triggered through change management rather than waiting for the next annual compliance meeting. Security and CMMC impact become part of architecture and procurement decisions.

NorthStar’s service transition process includes a CMMC impact field for customers that rely on its services for CUI protection. This makes compliance consequences visible before a platform is retired or a control is moved.

In practice, this is one of the areas where otherwise mature organizations can lose control of recognizing that major business or technology changes can alter the assumptions underlying certification. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of treat material change as a certification risk event is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to embed CMMC impact review into architecture, procurement, M&A, office moves, provider transitions, and security-platform changes. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include change tickets with CMMC impact, updated scope/SSP, control retests, and management disposition. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.38 Preserve the Assessment Record

After assessment, Harbor Point preserves the records it is responsible for under applicable retention, contractual, legal, and program requirements. The organization distinguishes official assessment records, its own evidence package, internal notes, provider records, and temporary working files.

Retention should be deliberate. Keeping every screen recording and duplicate export forever can create unnecessary security exposure. Deleting records casually can undermine future traceability. The retention matrix developed in Chapter 9 is applied to the assessment lifecycle.

Access to the archived assessment package is restricted. The fact that an artifact was shared during an assessment does not make it appropriate for broad internal distribution.

The operational significance of this section is easy to underestimate. It influences balancing traceability and future defensibility against unnecessary retention of

sensitive material. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of preserve the assessment record is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to classify official assessment records, internal evidence, provider records, working files, and temporary exports under explicit retention and access rules. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include a retention matrix, restricted archive, disposition records, legal-hold handling, and periodic access review. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.39 Conduct a Post-Assessment Lessons-Learned Review

Within a short period after the assessment, Harbor Point conducts a lessons-learned review while details are fresh. The review asks what caused delays, which evidence was difficult to retrieve, which interviews revealed knowledge gaps, which

demonstrations were fragile, which provider dependencies were poorly defined, and which documents were stale.

The output is a prioritized improvement backlog, not a narrative celebration. Items are assigned owners and dates. Easy improvements such as better evidence naming are distinguished from architectural issues such as overreliance on a provider capability that cannot produce customer-specific records.

NorthStar receives provider-specific action items and incorporates reusable improvements into its CMMC service model for other customers without disclosing Harbor Point confidential information.

A strong CMMC program treats this as a management discipline because it shapes converting assessment friction into measurable improvements to the operating model. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of conduct a post-assessment lessons-learned review is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore capture retrieval delays, stale documents, fragile demonstrations, interview knowledge gaps, and provider limitations while details are fresh. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include a prioritized lessons-learned backlog with owners, dates, recurrence potential, and service-design improvements. Those records should be customer-specific, current enough for the question being evaluated, and traceable

to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.40 Return Temporary Assessment Controls to Normal

Assessment preparation can create temporary accounts, conference bridges, screen-sharing permissions, evidence workspaces, guest access, and local working files. Harbor Point closes or removes them deliberately after they are no longer needed.

This cleanup is part of the assessment lifecycle. Forgotten guest accounts or broadly shared evidence folders can create new risk immediately after a successful assessment.

The assessment manager uses a closeout checklist covering accounts, links, shared folders, temporary firewall rules, test objects, exported evidence copies, visitor badges, and provider access changes.

This topic deserves more attention than a checklist item because it directly affects removing temporary conveniences before they become permanent security weaknesses. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of return temporary assessment controls to normal is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to close guest accounts, temporary shares, test objects, conference links, local exports, firewall exceptions, and special permissions after use. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility.

That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include a formal post-assessment cleanup checklist and verification of restored normal access. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.41 Define the MSP's Role Across the Lifecycle

NorthStar's role changes by phase. During readiness it can help analyze controls, remediate systems, build evidence, and test retrieval. During formal assessment it acts as a factual service provider and technical participant. During closeout it may implement corrective actions and provide evidence. During sustainment it monitors the services for which it is responsible and supports change impact reviews.

This role definition should be documented in the responsibility matrix and service agreement. Customers should know what assessment support is included, what requires separate professional services, how quickly evidence can be produced, and who can participate in assessor sessions.

Without a defined role, the MSP may be expected to function simultaneously as consultant, witness, administrator, project manager, and compliance guarantor. Those expectations are operationally dangerous.

During a formal assessment, the MSP should be a factual technical participant—not the customer's spokesperson and not an extension of the assessment team.

In practice, this is one of the areas where otherwise mature organizations can lose control of preventing the MSP from being treated as consultant, spokesperson, assessor, administrator, and guarantor at the same time. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of define the msp's role across the lifecycle is therefore not

administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to define what the MSP will prepare, demonstrate, remediate, retain, and support in each lifecycle phase. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include service descriptions, responsibility matrices, assessment-support runbooks, escalation terms, and commercial boundaries. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.42 Build Provider Assessment Support into Service Design

An MSP that serves defense-industrial-base customers should design services so customer-specific evidence and demonstrations are feasible. Multi-tenant platforms should support customer scoping, access logging, configuration reporting, and secure export when possible.

Service descriptions should identify evidence availability, retention limits, response times, support boundaries, subcontractor dependencies, and limitations. If a provider

cannot demonstrate a claimed security function at the customer level, the customer needs to understand that before relying on the service in its SSP.

NorthStar treats assessment support as an operational capability with runbooks, trained personnel, secure evidence procedures, and escalation paths rather than a favor performed by whichever engineer happens to be available.

The operational significance of this section is easy to underestimate. It influences making assessment support a repeatable service capability instead of emergency engineering. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of build provider assessment support into service design is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to design multi-tenant platforms, evidence retention, customer scoping, exports, logging, staffing, and escalation with DIB customers in mind. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include customer-specific reporting, evidence SLAs, trained support roles, tested runbooks, and documented platform limitations. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if

the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.43 Manage Communication with Executives

Executives need concise, decision-oriented information. Harbor Point uses an assessment dashboard that shows readiness gate status, assessment schedule, open scope issues, high-impact provider dependencies, evidence-request aging, significant assessment-day issues, conditional-status actions if any, and key lifecycle dates.

The dashboard avoids speculative score predictions. Before official results are available, management is told what evidence was requested, what operational issues were observed, and what risks require attention. This preserves accuracy and avoids unnecessary alarm.

After the assessment, the dashboard transitions to certification lifecycle status: official result, open closure actions, affirmation date, major change risks, and next certification window.

A strong CMMC program treats this as a management discipline because it shapes giving executives enough information to make decisions without speculative score forecasting. During post-assessment sustainment and provider operations, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of manage communication with executives is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore report readiness gates, open scope issues, provider risks, request aging, major decisions, conditional actions, and lifecycle dates in a concise dashboard. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from

becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include an executive dashboard linked to authoritative trackers and official results when available. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

Executive Assessment Dashboard

Dashboard element	Decision supported
Readiness gates	Proceed, remediate, or reschedule
Open scope questions	Boundary and contract implications
Provider dependencies	Escalation and lead-time risk
Evidence-request aging	Resource prioritization during assessment
Material changes	Need for SSP, scope, or evidence update
Lifecycle dates	Affirmation and next assessment planning

10.44 Harbor Point Case Study: Thirty Days Before Assessment

Thirty days before the scheduled assessment, Harbor Point’s readiness gate identifies three concerns. A recently added engineering application appears in the asset inventory but not the SSP diagram. NorthStar’s backup reporting retains only ninety days of detailed job records. A key HR interviewee will be traveling during the first assessment day.

The team updates scope analysis and confirms that the engineering application is in scope because it handles CUI. The SSP and diagram are revised through controlled change. NorthStar exports and preserves the needed backup history and updates the ongoing retention workflow. The assessment manager reschedules the HR interview and assigns a qualified backup participant.

None of these issues required panic because the readiness gate surfaced them with enough time for controlled correction.

This topic deserves more attention than a checklist item because it directly affects using the final month to surface cross-functional dependencies while there is still time for controlled correction. During case-study application and management review, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of harbor point case study: thirty days before assessment is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to treat each newly discovered asset, retention limit, unavailable interviewee, or provider dependency as a managed readiness issue. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include a 30-day readiness burn-down, updated scope records, preserved evidence, and confirmed participant coverage. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.45 Harbor Point Case Study: Assessment Day Two

On day two, an assessor asks how terminated users lose remote access. The HR coordinator explains the termination workflow, NorthStar shows the identity and VPN deprovisioning records for selected samples, and Harbor Point produces the reconciled termination population for the period.

During the demonstration, one historical ticket shows a delay between HR notification and account disablement. The team does not hide the record. It explains the incident, shows the documented exception handling, and provides the corrective action that was already implemented. The assessment team determines what that evidence means for the applicable requirement.

The important lesson is that mature assessment management does not depend on perfect-looking records. It depends on accurate evidence, traceability, accountable processes, and sustainable control implementation.

In practice, this is one of the areas where otherwise mature organizations can lose control of responding to imperfect historical records with transparency, context, and sustainable correction rather than concealment. During case-study application and management review, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of harbor point case study: assessment day two is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to coordinate HR, identity, VPN, ticketing, and MSP evidence so the assessor can see the real termination workflow and any exception history. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from

assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include sample-based records, exception documentation, corrective actions, and population reconciliation. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.46 Harbor Point Case Study: A Provider Limitation

Later, Beacon’s SOC portal cannot generate a customer-specific historical alert export for the requested period. The portal can display current alerts, but older records require Beacon operations to produce a report. This limitation was documented in the evidence index, so Harbor Point already has the escalation contact and expected turnaround.

The assessment coordinator opens the evidence request, Beacon generates the report through its controlled process, and Harbor Point receives it through the approved channel. The evidence note explains the provider-generated nature of the artifact and the period covered.

Because the dependency was understood before assessment, a platform limitation becomes a manageable evidence workflow rather than a surprise that disrupts the assessment.

The operational significance of this section is easy to underestimate. It influences handling service-provider limitations through known escalation and evidence paths. During case-study application and management review, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of harbor point case study: a provider limitation is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent

security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

In a shared-responsibility environment, this becomes workable only when the OSC and its providers agree to document what the platform can produce directly, what requires provider operations, expected turnaround, and how customer attribution is preserved. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

The validation question is not whether the team believes this is under control; it is whether the organization can demonstrate it consistently. For this section, the minimum evidence should include provider limitation records, escalation contacts, generated reports, delivery timestamps, and coverage notes. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.47 Harbor Point Case Study: Post-Assessment Transition

After the formal assessment activities conclude, Harbor Point does not immediately disband the team. It tracks clarification requests, protects the evidence workspace, preserves the decision log, and waits for the formal reporting process. When final status is achieved, the team records the certification lifecycle dates and conducts lessons learned.

The largest improvement item is not a failed security control. It is evidence retrieval latency. Several records required manual provider escalation. Harbor Point and NorthStar therefore automate selected customer-specific reports and extend preservation of recurring evidence.

This is an example of how an assessment can improve the operating model even when the organization’s primary goal is certification.

A strong CMMC program treats this as a management discipline because it shapes avoiding the common mistake of disbanding the team before reporting, cleanup, and lifecycle transition are complete. During case-study application and management review, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of harbor point case study: post-assessment transition is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

For an MSP-supported organization, the practical operating model should therefore retain a smaller closeout team to handle clarifications, records, lessons learned, automation opportunities, and certification calendar setup. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Management should expect objective proof that this process works under ordinary operating conditions, not only during assessment preparation. For this section, the minimum evidence should include closeout actions, preserved logs, improvement backlog, lifecycle dates, and evidence-automation changes. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.48 Common Assessment-Lifecycle Failures

Common failures include scheduling before scope is stable; assuming the SSP is current without reconciling it to architecture; relying on one employee for critical

knowledge; allowing evidence to move through uncontrolled email threads; exposing multi-tenant provider information; scripting interview answers; confusing policy with implementation; treating a dashboard as a substitute for source records; failing to prepare technical demonstrations; arguing determinations before all facts are clear; assuming every gap can be placed on a POA&M; and forgetting annual affirmation after certification.

Another common failure is assessment theater: temporary configuration changes, newly created records that imply a history that did not exist, or rehearsed explanations that conceal actual practice. This behavior undermines the integrity of the program and can create greater risk than the original control weakness.

The preventive pattern is consistent across these failures: establish ownership, use authoritative records, validate scope, manage change, preserve independence, and make the assessment reflect normal secure operations.

This topic deserves more attention than a checklist item because it directly affects recognizing recurring failure patterns early enough to prevent them. During case-study application and management review, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of common assessment-lifecycle failures is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

From the MSP perspective, the safest and most repeatable approach is to use assessment failures as design signals for governance, scope, evidence, provider contracts, staffing, and service architecture rather than isolated mistakes. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

A useful test is to ask whether a new employee or backup engineer could follow the process and reproduce the same result from the authoritative records. For this section, the minimum evidence should include a failure-pattern checklist, root-cause reviews, preventive controls, and recurring internal validation. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

10.49 Chapter Review and Readiness Questions

The assessment lifecycle connects governance, technology, evidence, people, providers, and formal certification processes. A strong program enters the assessment with stable scope, accurate documentation, tested evidence retrieval, prepared participants, safe demonstrations, and clear provider responsibilities. During the assessment it manages logistics without interfering with assessor independence. Afterward it treats reporting, closeout, annual affirmation, and change management as part of the same lifecycle.

Before moving to the next chapter, an MSP and its customer should be able to answer: Who owns the assessment calendar? Is the current C3PAO relationship documented and understood? Has scope been reconciled to the actual environment? Can every major provider produce customer-specific evidence? Are interviewees prepared to explain real work in their own words? Can technical controls be demonstrated safely? Is there a controlled request tracker? Does leadership understand conditional-status and affirmation obligations? Is there a process for material changes after certification?

If several answers are uncertain, the organization is not merely missing documentation. It has lifecycle-management work to complete.

In practice, this is one of the areas where otherwise mature organizations can lose control of testing whether the organization can explain and sustain the entire lifecycle without relying on last-minute heroics. During case-study application and management review, small ambiguities can propagate quickly: a person may make a decision based on an outdated assumption, a provider may deliver the wrong artifact, or a team may discover that an important dependency was never assigned. The purpose of chapter review and readiness questions is therefore not administrative neatness. It is to keep the assessment anchored to the same environment, responsibilities, and operating facts that the organization uses every day. When this

discipline is weak, the assessment team spends valuable time reconciling contradictions instead of evaluating a coherent security program. When it is strong, the organization can explain not only what it does, but why the process is controlled and how exceptions are handled.

The customer and its service providers should translate this principle into normal operations by choosing to use the review questions as management prompts for customer and MSP teams, then convert uncertain answers into owned work. This should be written into normal service delivery rather than held in the memory of one compliance lead. Harbor Point and NorthStar use the same principle throughout the chapter: the customer retains accountability for its CMMC status, while the MSP is accountable for the services, records, configurations, and explanations that fall within its assigned responsibility. That distinction keeps shared responsibility from becoming shared ambiguity. It also protects the MSP from being expected to certify facts outside its service boundary and protects the customer from assuming that outsourced administration automatically transfers regulatory accountability.

Sustainability is demonstrated when the same control, evidence, and decision path continues to work after the assessment calendar pressure disappears. For this section, the minimum evidence should include a chapter-end readiness assessment, action register, owners, dates, and cross-reference to the next lifecycle stage. Those records should be customer-specific, current enough for the question being evaluated, and traceable to an authoritative source. If an item cannot be produced without manual reconstruction, if two systems produce conflicting versions, or if only one person knows how to explain it, the team has identified a readiness weakness even if the underlying control appears technically enabled. The corrective action is to improve the operating process and evidence path, not merely to create a cleaner presentation for assessment week.

Assessment Lifecycle Checklist for MSP-Supported Organizations

- Confirm the assessment type, contract requirement, and authoritative CMMC sources currently applicable.
- Validate the C3PAO in the official Cyber AB ecosystem and review assessment contract terms.
- Reconcile SSP scope, asset inventory, network diagrams, locations, cloud services, security protection assets, specialized assets, and external service providers.
- Approve the assessment governance roster, decision rights, primary and backup contacts, and escalation paths.

- Test evidence retrieval from customer and provider systems, including historical records.
- Review evidence-sharing security, multi-tenant filtering, screen-sharing precautions, and temporary-access procedures.
- Prepare interviewees to explain actual processes without scripted answers.
- Rehearse technical demonstrations using safe production-representative methods and test objects where appropriate.
- Establish one evidence-request tracker and one controlled evidence-release process.
- Hold daily internal closeouts during active assessment activities.
- Capture factual corrections and material decisions in a controlled log.
- Understand scoring, conditional status, POA&M restrictions, and closeout obligations before the assessment begins.
- Preserve official and internal assessment records under the approved retention model.
- Close temporary assessment access and working repositories after they are no longer needed.
- Conduct lessons learned, update service runbooks, and schedule annual affirmation and next-cycle readiness activities.

Key Terms

Affirming Official: An individual authorized to affirm continuing compliance as required by the CMMC program.

Assessment Lifecycle: The end-to-end sequence from C3PAO selection and pre-assessment planning through conformity assessment, reporting, certification or POA&M closeout, affirmation, and sustainment.

C3PAO: CMMC Third-Party Assessment Organization authorized or accredited within the Cyber AB ecosystem to conduct applicable CMMC Level 2 certification assessments.

CAP: CMMC Assessment Process, the procedural framework used for Level 2 certification assessments.

Conditional Status: A time-limited CMMC status that may be available when regulatory scoring and POA&M conditions are satisfied.

Examine: An assessment method that reviews documents, records, configurations, and other artifacts.

Interview: An assessment method that obtains information from people with knowledge or responsibility for the implementation.

MET / NOT MET: Assessment determinations indicating whether the evaluated requirement satisfies the applicable criteria.

OSC: Organization Seeking Certification.

POA&M: Plan of Action and Milestones used to track permitted unresolved requirements under applicable program rules.

Test: An assessment method that exercises or observes a mechanism, process, or activity to verify behavior.

Official References

- 32 CFR Part 170, Cybersecurity Maturity Model Certification Program.
- Department of Defense, Defense Federal Acquisition Regulation Supplement provisions implementing CMMC requirements.
- NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information.
- Department of Defense, CMMC Level 2 Assessment Guide and applicable supplemental guidance.
- The Cyber AB, CMMC Assessment Process (CAP), current published version.
- The Cyber AB, official CMMC ecosystem and C3PAO information, including assessor and appeals processes.

Because CMMC implementation guidance and ecosystem procedures can change, readers should verify the current version of each source before using this chapter as an operational assessment checklist.

CMMC for MSPs

From Readiness to Certification

Chapter 11

Logging, Monitoring, and Security Operations

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and source context

11.1–11.7 Why logging and monitoring are operational controls, not product features

11.8–11.15 Designing the event pipeline: sources, collection, time, normalization, retention, and protection

11.16–11.24 Detection engineering: correlation, baselines, use cases, alert quality, and escalation

11.25–11.32 Security operations: triage, investigation, incident linkage, evidence preservation, and communications

11.33–11.38 MSP/MSSP shared responsibility, multi-tenant platforms, contracts, SLAs, and assessor evidence

11.39–11.43 Harbor Point security-operations case study, metrics, failure patterns, and sustainment

Security operations field guide, review questions, key terms, and official references

Chapter Purpose

Chapter 10 managed the CMMC assessment lifecycle. Chapter 11 turns from the assessment event to the operating reality that must exist before, during, and after any assessment: the ability to observe what is happening in the environment, recognize meaningful security activity, investigate it, preserve the necessary evidence, and act in time. Logging and monitoring are sometimes discussed as if they were synonymous with buying a SIEM, turning on an endpoint dashboard, or retaining firewall data. They are not. A mature security-operations capability is a chain of people, processes, technologies, decisions, and records. If any link is missing, the organization may possess large volumes of data without having reliable security visibility.

This distinction is especially important for managed service providers. An MSP may operate identity systems, endpoint protection, firewalls, backup platforms, remote-management tools, ticketing systems, cloud services, and security-monitoring infrastructure for multiple customers. Those platforms can give the provider unusually broad visibility, but they also create concentration risk and evidence complexity. A provider must know which events belong to which customer, which logs are authoritative, how long they are retained, who can alter them, how alerts are routed, what happens after hours, and how the customer can obtain records when an assessor or incident responder asks for them.

The Harbor Point Engineering case study continues in this chapter. NorthStar Managed Services administers key systems, while Beacon Security Operations provides managed detection and response. Harbor Point still retains responsibility for understanding its environment and making business decisions. The chapter follows the organizations as they build a defensible logging architecture, identify high-value event sources, establish customer-specific detection use cases, tune alerting, test escalation paths, preserve incident evidence, and demonstrate that monitoring is an operating process rather than a collection of screenshots.

CMMC requirements must be interpreted in the context of the governing regulation, applicable contract clauses, and the assessment framework in effect for the organization. As of September 2026, the Department has suspended Phase II CMMC requirements while Phase I self-assessment requirements remain in place. The underlying contractual safeguarding obligations, including applicable DFARS and NIST SP 800-171 requirements, continue to matter. This chapter therefore focuses on durable security operations that support both current obligations and future assessment readiness rather than designing a monitoring program around a single assessment date.

Learning Objectives

- Explain why audit logging, monitoring, detection, and security operations form a continuous control process rather than a single technology deployment.
- Map log sources to assets, identities, network boundaries, cloud services, security tools, applications, administrative platforms, and CUI workflows.
- Design reliable log collection that addresses time synchronization, normalization, transport, buffering, retention, access control, and integrity.
- Apply the NIST SP 800-171 Revision 2 Audit and Accountability requirements in an MSP-supported environment.
- Build detection use cases from realistic threat and operational scenarios rather than relying only on vendor-default alerts.
- Define triage, investigation, escalation, containment, incident-response, and evidence-preservation workflows.
- Manage false positives, alert fatigue, duplicated alerts, missing telemetry, and blind spots through controlled tuning and validation.
- Establish MSP/MSSP responsibilities for collection, monitoring, customer notification, evidence export, retention, and after-hours response.

- Produce assessor-ready evidence showing that logging and monitoring operate consistently over time.
- Measure security-operations effectiveness without confusing activity metrics with security outcomes.

Source and Program Context

The current CMMC program context remains in transition. The Department's July 13, 2026 announcement suspended Phase II requirements that had been scheduled to take effect on November 10, 2026, while keeping Phase I self-assessment requirements in place. Organizations should therefore verify current acquisition guidance before making certification-scheduling assumptions. The suspension does not turn logging, monitoring, incident response, or other safeguarding activities into optional practices. Those capabilities remain important to protecting CUI and to meeting contractual cybersecurity obligations where the relevant clauses apply.

For the Level 2 security baseline discussed throughout this book, NIST SP 800-171 Revision 2 remains central to the current Phase I enforcement posture described by the Department. Its Audit and Accountability family addresses the creation and retention of audit records, traceability to individual users, event review, alerting on audit failures, correlation, reduction and reporting, time synchronization, protection of audit information, and restriction of audit-management functions. Related requirements in System and Information Integrity and Incident Response connect monitoring to the detection of attacks, indications of compromise, unauthorized use, reporting, analysis, containment, recovery, and lessons learned.

The operational message for MSPs is straightforward: a customer cannot outsource the need to understand whether its security monitoring works. The provider may run the platform, but the customer and provider must be able to explain the sources being monitored, the events that matter, the retention and evidence path, the escalation process, and the division of responsibility. The remainder of this chapter translates those expectations into day-to-day operating practices.

11.1 Treat Logging as a Security Capability, Not a Storage Function

Logging is valuable only when recorded events can support accountability, detection, investigation, and decision-making. The first design question is therefore not how many gigabytes can be retained, but which events are necessary to reconstruct meaningful activity. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible

people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

For an MSP-supported environment, this topic must be designed around shared responsibility. The customer may not administer every platform, but it still needs enough visibility to understand what the provider is doing on its behalf. The provider, in turn, should avoid broad statements that are not tied to the customer's contracted service. A useful responsibility statement names the source, the collecting party, the monitoring party, the escalation recipient, the retention location, and the party that can produce evidence. If one of those fields is unknown, the organization has found an operational gap.

Harbor Point discovers that several systems retain logs locally, but no one has documented which events are collected centrally. NorthStar can show firewall and endpoint dashboards, yet identity and privileged-administration activity are only partially represented. The team creates a source-to-use-case map before expanding storage. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include source inventory, event-selection standard, sample records, central-collection status, owners. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

Management should review this area through risk and service outcomes, not technology branding. A monitoring platform can be powerful and still be poorly configured for the customer's environment. Conversely, a modest toolset can provide defensible visibility when sources are selected deliberately, responsibilities are clear, events are retained appropriately, detections are tested, and escalation works. The

goal is dependable security operations that protect the environment every day, with assessment evidence being a natural by-product of that discipline.

11.2 Connect Monitoring to the CUI Workflow

Security visibility should follow the path of CUI through people, endpoints, applications, repositories, networks, cloud services, backups, and support systems. Monitoring that is disconnected from the CUI workflow can be technically impressive while missing the systems that matter most. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

The Harbor Point team walks one engineering file from receipt through editing, collaboration, storage, backup, and external transfer. That exercise reveals a cloud sharing service and a service account that were not in Beacon's primary detection scope. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include CUI data-flow map, asset inventory, log coverage overlay, identified gaps, remediation tickets. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.3 Define Authoritative Sources

The same event may appear in several systems, and those systems may disagree. A monitoring program needs to identify which source is authoritative for identity, device state, network connection, administrative change, alert disposition, and incident status. In practice, the objective is to create a process that can be explained

and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

NorthStar's RMM records a patch action while the endpoint platform records a process launch and the ticketing system records the approved maintenance. Harbor Point documents which system proves approval, which proves execution, and which proves device outcome. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include authoritative-source matrix, system owners, clock source, field definitions, reconciliation procedure. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.4 Build Accountability into Event Design

Audit records should make it possible to associate actions with individual users, privileged accounts, service identities, devices, and administrative sessions to the extent technically feasible. Shared credentials and generic administrative identities weaken that chain. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point eliminates a shared help-desk administrator account and requires named privileged accounts for NorthStar technicians. Beacon then adjusts detections so privileged actions can be tied to a person and customer ticket. The team then asks a

validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include named-account policy, privileged-account roster, authentication logs, session logs, change tickets. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.5 Select Events Deliberately

Collecting everything is rarely a practical strategy. Event selection should begin with security requirements, threat scenarios, system criticality, business workflows, incident-response needs, and the ability to investigate high-risk activity. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

The team prioritizes authentication failures, successful privileged sign-ins, account changes, group membership changes, security-tool tampering, remote-access events, firewall denies, unusual outbound traffic, malware detections, backup administration, and CUI repository access. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include event catalog, rationale, severity, source, owner, retention target, use-case mapping. The strongest records are customer-specific, dated,

traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.6 Recognize Monitoring Blind Spots

A blind spot is not merely a device that does not send logs. It can be an unmanaged account, a SaaS application without export capability, an encrypted channel that bypasses inspection, a provider platform that hides tenant detail, or an event field lost during normalization. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon demonstrates excellent endpoint visibility but cannot see administrative activity inside one legacy SaaS application. Harbor Point records the limitation, restricts administration, enables the vendor's enhanced audit feature, and creates a manual review until automated collection is available. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include coverage assessment, blind-spot register, compensating process, vendor capability record, closure validation. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.7 Separate Availability Monitoring from Security Monitoring

Operational monitoring asks whether systems are up, responsive, and within capacity. Security monitoring asks whether activity is authorized, expected, and potentially harmful. The two overlap, but neither substitutes for the other. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

NorthStar's network monitor reports that the VPN gateway is healthy while Beacon identifies repeated impossible-travel authentication attempts. The first confirms availability; the second investigates misuse. Harbor Point keeps both workflows linked but distinct. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include NOC/SOC responsibilities, alert-routing matrix, escalation thresholds, joint runbook, sample incidents. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.8 Create a Log-Source Inventory

A defensible log program begins with an inventory that connects each source to an asset, owner, collection method, event types, retention location, and monitoring use cases. Without that inventory, gaps emerge silently as systems change. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning.

This is the difference between a control that exists on paper and a control that can withstand technical review.

NorthStar exports the asset inventory and compares it with Beacon's active log connectors. Several switches, a backup console, and an administrative jump host are missing. The mismatch becomes a tracked remediation workstream. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include log-source inventory, asset reconciliation, connector status, gap list, review date. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.9 Design Reliable Collection Paths

Collection architecture should account for agents, APIs, syslog, cloud connectors, collectors, queues, network interruptions, authentication, encryption, and retry behavior. The design should fail visibly rather than losing events silently. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point's cloud identity connector stops after a certificate rollover. Beacon's platform raises a source-health alert, but the customer notification rule is missing. The revised design treats loss of telemetry as a security event with an owner and escalation path. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective

action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include architecture diagram, connector configuration, health alerts, buffering settings, failure tests. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.10 Synchronize Time

Correlation depends on consistent time. Systems should use reliable time sources, record time zones or offsets consistently, and account for devices that drift or applications that store local time. Investigations become unreliable when timestamps cannot be aligned. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

During a Harbor Point test, firewall events appear seven minutes earlier than endpoint activity because a legacy appliance is not synchronized. NorthStar corrects the time source and documents a periodic check for drift. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include time-source configuration, NTP settings, drift checks, sample correlated events, exception record. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that

hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.11 Normalize Without Destroying Meaning

Normalization helps analysts compare events across technologies, but transformations can remove vendor-specific detail. The monitoring architecture should preserve raw records when feasible while creating normalized fields for search and correlation. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon maps user, source IP, destination, action, device, and event category into common fields. It also retains the original payload so an investigator can verify details that the parser did not expose. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include parsing rules, field mapping, raw-log retention, parser version, validation samples. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.12 Protect Logs in Transit and at Rest

Audit information can become evidence. Collection channels, storage, administrative access, and export mechanisms should be protected against unauthorized disclosure, alteration, and deletion. Monitoring infrastructure should not become an easier path to sensitive data. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people,

the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

NorthStar separates log-administration roles from normal help-desk roles and uses encrypted transport from key collectors. Beacon limits customer analysts to Harbor Point's tenant data and logs administrative actions within the monitoring platform. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include encryption configuration, access-control lists, role assignments, administrative audit logs, export controls. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.13 Control Audit-Management Privileges

The ability to disable logging, change retention, delete records, modify parsers, suppress alerts, or alter detection rules is powerful. Those actions should be restricted, reviewed, and attributable. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon requires elevated approval for disabling a Harbor Point log source or detection. NorthStar's engineers can request changes but cannot silently change the MSSP's customer alert rules. Emergency actions are documented and retrospectively reviewed. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an

undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include privileged-role matrix, approval workflow, change history, emergency procedure, periodic review. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.14 Set Retention from Real Requirements

Retention should be based on contractual obligations, incident-response needs, threat-detection use cases, investigation timelines, legal considerations, and storage constraints. A single default retention period may not fit every source. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point classifies log categories by investigative value. Identity, endpoint, privileged administration, firewall, and CUI repository records receive higher-priority retention than low-value operational telemetry. The schedule is documented and reviewed with counsel and contracts personnel as appropriate. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include retention schedule, rationale, platform settings, storage reports, disposal procedure. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also

show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.15 Monitor the Monitoring System

Telemetry pipelines can fail. A mature program measures source health, ingestion delay, parser errors, dropped events, license or capacity limits, and changes in expected event volume. Silence should be investigated, not assumed to mean safety. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon creates daily health checks and alerts for sudden drops in authentication and endpoint events. A 90-percent decrease from a critical source becomes a service incident even if the SIEM itself remains online. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include source-health dashboard, ingestion metrics, failure alerts, ticket history, monthly service review. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.16 Build Detection Use Cases from Scenarios

Detection engineering starts with behaviors that matter: credential theft, unauthorized privilege, persistence, suspicious remote administration, data staging, abnormal transfer, malware, security-tool tampering, and other patterns relevant to the environment. In practice, the objective is to create a process that can be explained and

reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point's first use-case workshop begins with how an attacker could misuse NorthStar's remote-management access. The team defines expected technician behavior, approved maintenance windows, source networks, ticket correlation, and escalation triggers. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include use-case catalog, threat scenario, data prerequisites, logic, severity, response action. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.17 Establish a Baseline of Normal Activity

Baselines help distinguish expected administration from unusual behavior. They should be treated as analytical context rather than automatic proof that activity is safe. Business changes, travel, maintenance, and new applications can change normal patterns. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon profiles typical privileged sign-in locations, service-account schedules, remote-management hours, backup activity, and large file transfers. Exceptions are reviewed with Harbor Point rather than simply suppressed. The team then asks a

validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include baseline report, approved exceptions, business context, tuning history, review cadence. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.18 Correlate Across Identity, Endpoint, Network, and Cloud

Single events often have low confidence. Correlation can combine authentication, device, process, network, cloud, and administrative context to create a stronger signal. The design should document which sources are necessary for each use case. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

A successful sign-in from a new country is not automatically an incident. When it is followed by an endpoint token event, privileged group change, and outbound archive transfer, Beacon raises the priority and opens an investigation. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include correlation logic, source dependencies, test data, alert record, investigation timeline. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case,

configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.19 Detect Privileged-Access Misuse

Privileged activity deserves focused monitoring because administrative credentials can change security settings, access data, create persistence, or disable visibility. MSP environments add remote support and cross-customer administration to this risk. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

NorthStar uses separate technician identities and a controlled administrative path for Harbor Point. Beacon alerts on first-time privilege use, unusual source location, after-hours high-risk changes, new administrator creation, and security-tool disablement. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include privileged access logs, PAM/RMM records, ticket correlation, detection rules, review evidence. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.20 Monitor Remote Management and RMM Platforms

RMM and remote-support platforms are operationally valuable but high-impact. Monitoring should address sign-ins, new agents, script execution, policy changes, credential changes, file transfer, remote shell activity, and unusual cross-tenant

behavior. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point requires NorthStar to provide customer-specific RMM audit exports. Beacon ingests selected events and correlates high-risk technician actions with change tickets. NorthStar also monitors its own platform for provider-level compromise. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include RMM audit logs, tenant filters, admin events, platform security alerts, change tickets. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.21 Monitor Identity and Authentication Signals

Identity telemetry often provides the earliest indication of account compromise. Useful signals include failed and successful authentication, MFA outcomes, password resets, token issuance, device registration, conditional-access events, and privilege changes. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon creates a Harbor Point identity dashboard that highlights risky sign-ins, repeated MFA denial patterns, new device registrations, legacy authentication

attempts, and administrative changes. The dashboard supports investigation but does not replace case handling. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include identity logs, MFA records, conditional-access events, account-change audit, case examples. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.22 Monitor Endpoints and Servers

Endpoint and server visibility should support malware detection, process analysis, persistence discovery, security-control health, account activity, configuration changes, and investigation. Coverage should be reconciled to the in-scope asset inventory. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

NorthStar compares Harbor Point's asset list with Beacon's EDR console each month. Missing agents, stale devices, disabled sensors, and unsupported operating systems are treated as monitoring gaps rather than inventory trivia. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include EDR inventory, health status, policy assignment, alert

history, gap tickets. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.23 Monitor Network Boundaries and Communications

Network telemetry can provide context that endpoint tools miss. Firewalls, secure web gateways, DNS, VPN, proxies, network detection systems, and selected flow or packet data can support detection and investigation when configured with clear purposes. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point retains firewall and VPN events and sends high-value records to Beacon. DNS events are added for malware and command-and-control investigation. Full packet capture is not collected everywhere; the architecture documents where deeper network evidence is available. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include firewall logs, VPN records, DNS logs, IDS/NDR alerts, architecture diagram. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.24 Monitor Cloud and SaaS Administration

Cloud services may hold CUI, protect in-scope systems, or provide security functions. Their audit capabilities vary by subscription and offering. Monitoring design should verify tenant-level logging, administrative actions, exports, APIs, and retention. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

A Harbor Point SaaS platform originally retains only a short audit window. NorthStar enables the appropriate logging capability and Beacon collects administrative events. The contract record documents the dependency and export method. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include tenant audit settings, API connector, admin events, retention evidence, provider documentation. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.25 Design Triage as a Repeatable Process

Triage determines whether an alert is benign, expected, suspicious, or incident-worthy. Analysts need context, decision criteria, access to supporting data, and a documented way to record what was reviewed and why a disposition was made. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning.

This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon's triage record captures alert source, affected customer, identity, asset, timeline, enrichment, analyst conclusion, severity, escalation decision, and linked evidence. Harbor Point can review closed cases during service governance. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include triage SOP, case template, sample closed alerts, analyst notes, quality review. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.26 Use Severity and Priority Carefully

Alert severity describes technical or security significance; operational priority also considers customer context, CUI exposure, asset criticality, privilege, business impact, and timing. A vendor's default severity should not automatically determine response. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

A medium vendor alert on Harbor Point's engineering repository is escalated because it involves a privileged account and unusual data access. A high-severity test event from an approved exercise is closed with documented context. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the

process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include severity matrix, customer priorities, asset criticality map, escalation criteria, case records. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.27 Control Alert Fatigue

Excessive low-value alerts reduce attention and can cause meaningful activity to be overlooked. Tuning should remove noise without hiding risk. Every suppression or threshold change should have a reason, owner, test, and review date. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon finds that a backup service account produces hundreds of predictable failed logons during a legacy task. Instead of globally suppressing authentication failures, the team corrects the task and narrows a temporary exception. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include tuning register, suppression rules, before/after metrics, approval, expiration date. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source

failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.28 Escalate with Clear Time and Ownership Expectations

Security operations fail when everyone can see an alert but no one is obligated to act. Escalation matrices should define who is contacted, how quickly, by which method, after what threshold, and what happens when the primary contact is unavailable. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point identifies a primary and backup incident contact. Beacon's runbook distinguishes advisory notifications from urgent security escalations. NorthStar receives technical actions through a controlled ticket while Harbor Point retains incident authority. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include contact matrix, SLA, call tree, escalation test, after-hours procedure. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.29 Link Monitoring to Incident Response

Monitoring should feed directly into incident response. A high-confidence alert may require containment, evidence preservation, contractual reporting analysis, management notification, legal review, and recovery actions. The transition from alert to incident should be explicit. In practice, the objective is to create a process that

can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon escalates suspicious credential misuse. Harbor Point opens its incident process, NorthStar isolates the endpoint under authorization, and the team preserves relevant records. The incident commander, not the monitoring analyst, coordinates broader business decisions. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include IR plan, alert-to-incident criteria, incident record, containment authorization, communications log. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.30 Preserve Evidence Before It Disappears

Some evidence is volatile or subject to short retention. Incident workflows should identify what must be preserved, who is authorized to collect it, how integrity is maintained, and where it is stored. Contractual preservation obligations must be considered when applicable. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

For a suspected compromise, Harbor Point preserves relevant system images and monitoring data under its incident process. Where DFARS 252.204-7012 applies, the organization evaluates the clause's reporting and preservation requirements rather

than relying solely on routine SIEM retention. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include preservation checklist, chain-of-custody record, exported logs, hashes where used, incident timeline. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.31 Investigate Across Systems, Not in Isolation

Investigations should reconstruct activity across identity, endpoint, network, cloud, application, ticketing, and provider systems. Analysts need a method for aligning time, identities, assets, and events while distinguishing facts from hypotheses. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon builds a timeline showing a suspicious sign-in, remote command, process execution, outbound connection, and administrative ticket history. Harbor Point can see which facts came from which source and where uncertainty remains. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include timeline, source citations, analyst notes, supporting records, unresolved questions. The strongest records are customer-specific, dated, traceable to

an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.32 Close Cases with Learning, Not Just Disposition

Case closure should capture why an event occurred, whether a control failed, whether a detection should be changed, and whether documentation or training needs correction. Repeated benign alerts may indicate poor tuning; repeated true events may indicate a control weakness. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

After three similar remote-access alerts, Harbor Point discovers that an approved vendor workflow bypasses the documented access path. The team fixes the workflow and updates monitoring rather than repeatedly closing the same alert as expected activity. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include closure criteria, root-cause note, corrective action, rule update, lessons learned. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.33 Define MSP, MSSP, and Customer Responsibilities

Shared responsibility must be explicit. The customer, MSP, MSSP, cloud provider, and software vendors may each control different parts of the evidence and response

chain. Responsibility should be assigned for collection, retention, monitoring, notification, investigation, action, and export. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point owns incident authority and business decisions. NorthStar owns specified infrastructure administration and source-health remediation. Beacon owns continuous monitoring, first-line triage, and escalation for contracted sources. The responsibility matrix also identifies dependencies on cloud vendors. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include responsibility matrix, service description, RACI, escalation map, provider evidence list. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.34 Design Multi-Tenant Security Operations Safely

MSP and MSSP platforms often serve many customers. Tenant isolation, analyst permissions, data labeling, export controls, customer context, and cross-tenant administrative activity should be designed so one customer's records are not exposed or confused with another's. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon requires customer-specific case identifiers and tenant-scoped analyst access. NorthStar's automation includes the customer context in administrative actions. Quality review checks that exported evidence contains only Harbor Point information. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include tenant controls, role assignments, case labels, export procedure, access review. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.35 Put Evidence Rights into Contracts and Service Design

An organization should not discover during an assessment or incident that its provider cannot produce the needed records. Service agreements should address log availability, retention, export format, response times, support for investigations, and known platform limitations. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point's service schedule requires NorthStar and Beacon to provide specified customer records within defined timeframes. It also documents which provider-level records cannot be shared directly and what customer-specific alternatives are available. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective

action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include contract/SOW language, evidence SLA, data ownership terms, export examples, limitation register. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.36 Test After-Hours Security Operations

Attackers do not respect business hours. If the organization relies on monitoring outside normal working time, it should test the actual escalation path, not merely confirm that a service is marketed as 24x7. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point runs an after-hours exercise. Beacon reaches the backup contact, NorthStar confirms isolation authority, and management receives the expected notification. A failed phone number is corrected before a real incident occurs. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include exercise record, contact test, escalation timestamps, corrective actions, retest. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.37 Prepare Monitoring Evidence for Assessment

Assessment evidence should show operation over time. Useful material includes source inventories, architecture diagrams, retention configurations, event samples, alert records, triage cases, tuning history, source-health reports, access reviews, escalation tests, and incident records where appropriate. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Instead of presenting a single SIEM screenshot, Harbor Point prepares an evidence path showing how one use case is sourced, detected, triaged, escalated, and closed. The assessor can trace the process from configuration to operational record. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include evidence index, screenshots with context, exported records, tickets, policies, interviews. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.38 Avoid Overclaiming Provider Capabilities

A contract or marketing statement that says '24x7 SOC' or 'CMMC ready' does not prove that the customer's required sources are monitored or that the evidence is retrievable. Claims should be verified against configuration and actual service behavior. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually

functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point asks Beacon to demonstrate which sources are active for its tenant, how a high-risk alert is handled, what data is retained, and how records are exported. The result is compared with the responsibility matrix and SSP. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include service validation, tenant configuration, test alert, export demonstration, responsibility reconciliation. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.39 Harbor Point Case Study: Build the Coverage Baseline

The case study begins with reconciliation rather than assumptions. Harbor Point compares the CUI workflow, asset inventory, NorthStar management systems, Beacon connectors, and cloud services to build one monitoring baseline. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

The first pass finds strong endpoint and firewall coverage, partial identity correlation, missing backup administration logs, inconsistent RMM ticket correlation, and one SaaS audit limitation. Each gap is assigned an owner and validation method. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider

practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include coverage matrix, gap register, owner list, validation plan, management summary. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.40 Harbor Point Case Study: Engineer and Test Detections

The team selects high-value scenarios based on privileged access, remote administration, suspicious authentication, security-tool tampering, malware, and unusual data movement. Each rule is tested using controlled events or representative records. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Beacon records expected inputs, logic, severity, notification, and evidence for each use case. NorthStar verifies that legitimate maintenance does not create unmanageable noise and that emergency actions remain visible. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include use-case tests, alert screenshots, case records, tuning history, approval. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or

unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.41 Harbor Point Case Study: Exercise the Escalation Chain

A monitoring capability is incomplete until the alert reaches a person who can make or authorize the required decision. Harbor Point therefore runs a tabletop and a technical alert simulation. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

The test measures detection, triage, notification, customer acknowledgement, technical containment authorization, evidence export, and management communication. The team corrects contact and workflow weaknesses before declaring the process mature. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include exercise plan, timestamps, participant record, lessons learned, corrective actions. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.42 Measure Security Operations with Balanced Metrics

Metrics should reveal whether the monitoring system is healthy and whether people can act effectively. Useful measures include source coverage, ingestion health, alert volume by use case, acknowledgement time, escalation time, repeated false positives, unresolved cases, and evidence-delivery performance. In practice, the objective is to create a process that can be explained and reproduced. The organization should be

able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point's dashboard avoids treating a lower alert count as automatic proof of improvement. It combines coverage, quality, timeliness, and corrective-action data so management can distinguish reduced risk from reduced visibility. The team then asks a validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include dashboard, metric definitions, trend report, service review minutes, corrective decisions. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

11.43 Sustain Monitoring as the Environment Changes

New systems, cloud services, acquisitions, provider changes, network redesigns, software upgrades, account models, and business processes can invalidate the monitoring baseline. Change management should include a security-visibility impact review. In practice, the objective is to create a process that can be explained and reproduced. The organization should be able to identify the responsible people, the systems that produce the records, the location of the authoritative configuration, the expected operating cadence, and the evidence that shows the process is actually functioning. This is the difference between a control that exists on paper and a control that can withstand technical review.

Harbor Point adds a monitoring-impact question to technology and provider changes: what new events are created, what sources are retired, how retention changes, which detections are affected, and what evidence path must be updated. This converts monitoring from a project into an operating discipline. The team then asks a

validation question: could a different engineer, analyst, or assessor follow the records and reach the same factual conclusion? If the answer depends on one person's memory, a temporary dashboard state, or an undocumented provider practice, the process is not yet mature enough. The corrective action is to improve the operating path rather than to create a one-time assessment artifact.

Assessment readiness should emerge from ordinary operations. Useful evidence for this section can include change records, monitoring impact assessment, updated diagrams, connector changes, post-change validation. The strongest records are customer-specific, dated, traceable to an authoritative system, and connected to a policy, procedure, ticket, case, configuration, or test that explains why the record exists. Evidence should also show exceptions and corrective actions; a perfect-looking dashboard that hides source failures or unresolved cases can be less credible than a controlled process that detects, documents, and fixes them.

Security Operations Field Guide

The field guide below condenses the chapter into practical checkpoints that an MSP and customer can use during implementation, service review, internal readiness work, or preparation for an assessment. It is not a substitute for the governing requirements; it is a way to organize the operating questions that should already have answers.

Area	Operational Question	Typical Evidence
Coverage	Do all in-scope assets, identities, administrative platforms, cloud services, and security protection systems have an intentional monitoring decision?	Coverage matrix; reconciled inventories
Collection	Are connectors healthy, authenticated, encrypted as appropriate, buffered, and monitored for failure?	Architecture; source-health reports; failure tests
Time	Can events from different sources be aligned reliably?	NTP/time settings; correlation test
Integrity	Who can alter, delete, suppress, or change audit data and rules?	RBAC; privileged access review; change history
Retention	Is retention defined by source and justified by operational and contractual needs?	Retention schedule; storage settings
Detection	Are use cases tied to realistic	Use-case catalog; test alerts; tuning

	scenarios and tested?	history
Triage	Do analysts record what they reviewed and why they closed or escalated an alert?	Case templates; quality review
Escalation	Are customer contacts, time expectations, and after-hours paths tested?	SLA; call tree; exercise results
Incident Linkage	Is there a clear threshold for turning an alert into an incident process?	IR plan; escalation criteria; incident records
Evidence	Can the customer obtain customer-specific records without manual reconstruction?	Evidence SLA; exports; retrieval test
Change	Do system/provider changes trigger a monitoring impact review?	Change tickets; post-change validation
Governance	Do management and service owners review health, quality, and corrective actions?	Service review minutes; dashboard; action log

Common Failure Patterns

Failure Pattern	**Why It Matters**
Buying a SIEM without defining what must be detected	The platform becomes a storage destination rather than a security capability.
Collecting logs without source-health monitoring	A connector can fail for weeks while dashboards continue to look normal.
Treating vendor-default rules as the detection strategy	Alerts may not reflect customer-specific threats, privileged workflows, or CUI use.
Using shared administrator accounts	Actions cannot be attributed reliably to individual technicians.
Suppressing noisy alerts without governance	Tuning can silently hide meaningful activity.
Retaining only dashboard views	Screenshots may not preserve the detail needed for investigation or assessment.
Assuming the MSSP owns incident response	Monitoring and triage do not automatically transfer customer business authority or contractual duties.
Ignoring RMM and provider administrative logs	The highest-impact support path may become a monitoring blind spot.
Failing to reconcile assets and log sources	Unmonitored systems can disappear from the visibility model.

Testing during business hours only	After-hours contacts and authority gaps remain undiscovered until an actual incident.

Management Review Checklist

- Confirm that the log-source inventory has been reconciled with the current in-scope asset and service inventory.
- Review source-health exceptions, ingestion delays, parser failures, and unresolved telemetry gaps.
- Review privileged-administration, RMM, identity, endpoint, firewall, VPN, cloud, and CUI-repository coverage.
- Confirm that high-value detection use cases have been tested and that tuning changes are documented.
- Review alert aging, escalations, open investigations, repeated false positives, and recurring root causes.
- Confirm that primary and backup customer contacts are current and that after-hours escalation has been tested.
- Verify that provider evidence can be exported in a customer-specific form within the agreed timeframe.
- Review any system, provider, architecture, or business change that may have altered the monitoring baseline.
- Confirm that incident-response and contractual reporting procedures are linked to monitoring escalation.
- Record management decisions, accepted limitations, corrective actions, owners, and target dates.

Review Questions

1. Why is logging not the same thing as security monitoring?
2. How should the CUI workflow influence log-source selection?
3. What is an authoritative event source, and why should it be documented?
4. Why do shared administrator accounts weaken audit accountability?
5. What factors should drive event selection?
6. Give three examples of monitoring blind spots that do not involve a completely unlogged device.
7. How does availability monitoring differ from security monitoring?

8. What fields should a log-source inventory contain?
9. Why should collection-pipeline failure generate an alert?
10. Why is reliable time synchronization important to investigations?
11. What is the benefit of preserving raw events when data is normalized?
12. Why must audit-management privileges be restricted?
13. How should log retention periods be determined?
14. What source-health metrics can reveal silent telemetry loss?
15. What makes a detection use case stronger than a vendor-default rule?
16. How should a baseline of normal activity be used without treating normal as automatically safe?
17. Why is cross-source correlation valuable?
18. What privileged-access events are especially important in MSP environments?
19. Why should RMM platforms receive focused monitoring?
20. What identity events can provide early evidence of account compromise?
21. How should endpoint-monitoring coverage be reconciled to the asset inventory?
22. What network records can support security investigations?
23. What cloud-service characteristics should be verified before relying on provider audit logs?
24. What information should a triage record preserve?
25. Why should operational priority differ from vendor alert severity?
26. What risks arise from uncontrolled alert suppression?
27. What should an escalation matrix specify?
28. How should monitoring connect to the incident-response process?
29. Why can routine SIEM retention be insufficient during a contractual cyber incident?
30. What should a cross-system investigation timeline distinguish?
31. What should happen after a case is closed?
32. Which logging and monitoring responsibilities should be divided among customer, MSP, and MSSP?
33. What special risks arise from multi-tenant monitoring platforms?
34. What evidence rights should be addressed in service contracts?
35. Why should after-hours escalation be tested?
36. What makes monitoring evidence persuasive during assessment?

37. Why is a provider marketing statement not sufficient proof of customer monitoring coverage?

38. What did Harbor Point learn by reconciling the CUI workflow, asset inventory, and monitoring connectors?

39. How should detection rules be tested?

40. What does an escalation exercise reveal that documentation alone cannot?

41. Which metrics help management distinguish reduced risk from reduced visibility?

42. Why should technology changes trigger a monitoring-impact review?

Answer Guidance

Questions 1 through 7 focus on the purpose and scope of monitoring. A technically large collection of logs is not automatically useful. The organization should know what it needs to observe, why each source matters, how activity can be attributed, and how visibility follows the CUI workflow. Availability data and security data can support one another, but they answer different questions.

Questions 8 through 14 focus on pipeline reliability and audit protection. Collection, time synchronization, normalization, access control, retention, and source-health monitoring determine whether audit records can be trusted when they are needed. A mature environment detects missing telemetry and administrative changes to the monitoring system instead of assuming that silence means there is no problem.

Questions 15 through 23 focus on detection engineering. Effective use cases combine threat scenarios, customer context, source dependencies, and tested logic. Identity, endpoint, network, cloud, privileged administration, and RMM data are especially valuable when the organization correlates them rather than reviewing them as isolated dashboards.

Questions 24 through 31 focus on security operations. Triage, severity, tuning, escalation, incident linkage, evidence preservation, investigation, and lessons learned should form one controlled workflow. Documentation should preserve factual reasoning so that another analyst can understand how the decision was made.

Questions 32 through 42 focus on provider responsibility and sustainment. MSP and MSSP services should define tenant isolation, evidence rights, notification expectations, after-hours support, assessment assistance, and change impact. Harbor Point's case study demonstrates that the operational test is not whether a provider says the service exists, but whether the customer can verify that the correct sources are monitored and that people can act on the results.

Key Terms

Term	Meaning
Alert fatigue	Loss of analyst effectiveness caused by excessive or low-value alerts.
Audit record	Recorded information about an event or action that supports accountability, analysis, or investigation.
Authoritative source	The system or record designated as the primary source for a specific fact or event type.
Baseline	A documented representation of expected activity used as context for detecting meaningful deviation.
Correlation	Combining related events or context from multiple sources to create a stronger analytical conclusion.
Detection use case	A defined scenario, data requirement, logic, severity, and response path for identifying suspicious activity.
EDR	Endpoint Detection and Response technology used to collect endpoint telemetry and detect or investigate threats.
Event normalization	Mapping differently formatted source events into common fields while preserving necessary meaning.
False positive	An alert that appears suspicious under detection logic but is determined to be benign or expected.
Ingestion delay	The time between event creation and availability in the monitoring platform.
MDR	Managed Detection and Response service that provides monitoring, detection, investigation, and often response support.
MSSP	Managed Security Service Provider.
NOC	Network Operations Center, generally focused on service availability and operational health.
RMM	Remote Monitoring and Management platform used by service providers for administration and support.
SIEM	Security Information and Event Management platform used to collect, search, correlate, and analyze security events.
SOC	Security Operations Center.
Source health	The operational condition of a telemetry source or connector, including whether events are arriving as

	expected.
Telemetry	Security-relevant data produced by systems, users, networks, applications, and security tools.
Triage	The initial review and classification of an alert to determine significance and next action.
Use-case tuning	Controlled adjustment of detection logic, thresholds, exclusions, or context to improve signal quality.

Official References

R1. Department of War Chief Information Officer. Cybersecurity Maturity Model Certification (CMMC) program pages and current program status. The July 13, 2026 announcement suspended Phase II requirements while Phase I self-assessment requirements remain in place. Review current official guidance before relying on implementation dates.

R2. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Use the current edition and applicable provisions for scope, assessment, external service providers, affirmation, and related program requirements.

R3. National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Although NIST has published Revision 3, current CMMC Phase I enforcement guidance referenced by the Department continues to center on Revision 2 at the time of this chapter.

R4. National Institute of Standards and Technology. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information. Use the applicable assessment procedures associated with the governing CMMC/contractual baseline.

R5. Defense Federal Acquisition Regulation Supplement 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Review the current clause and the organization's actual contract for safeguarding, reporting, preservation, cloud-service, and flow-down obligations.

R6. Applicable customer contracts, provider service descriptions, statements of work, incident-response procedures, and monitoring architecture records. Contract-specific obligations can be more important than generic service assumptions.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance. It does not replace the governing regulation, an applicable solicitation or contract, legal advice, or an authorized CMMC assessment.

Chapter Closing Perspective

Logging and monitoring are often invisible when they work well. The organization sees a normal business day, while underneath that day thousands or millions of events are being generated, transported, parsed, correlated, reviewed, and retained. The value of the security-operations program appears when something changes: a credential is misused, an endpoint behaves unexpectedly, a provider account performs an unusual action, a security tool stops reporting, or an incident requires the team to reconstruct what happened.

For an MSP, the standard is higher than simply owning a powerful platform. The provider must be able to operate that platform in a customer-specific, accountable, and retrievable way. The customer must understand what it receives and what remains its responsibility. When those responsibilities are explicit, telemetry is healthy, detections are tested, alerts are triaged, escalation works, and evidence can be produced, monitoring becomes more than a compliance artifact. It becomes part of the organization's ability to protect CUI and recover from security events.

Harbor Point's progress in this chapter illustrates the larger theme of the book: readiness is created by disciplined operations. The strongest assessment evidence is generated by a process that people actually use. Chapter 12 can now build on that operational visibility by focusing on incident response, cyber-event handling, and the coordinated actions that follow when monitoring indicates that something has gone wrong.

CMMC for MSPs

From Readiness to Certification

Chapter 12

Vulnerability, Configuration, and Patch Management

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Contents

Purpose, learning objectives, and September 2026 source context

12.1–12.8 Building the vulnerability and configuration-management foundation

12.9–12.16 Secure baselines, configuration drift, and controlled change

12.17–12.24 Vulnerability discovery, validation, prioritization, and ownership

12.25–12.32 Patch planning, testing, deployment, verification, and exceptions

12.33–12.40 MSP operating models, cloud and specialized assets, metrics, and evidence

12.41–12.48 Harbor Point case study, workshops, field guide, failures, and sustainment

Implementation checklist, review questions, answer guidance, key terms, and official references

Chapter Purpose

Chapter 11 established how an MSP-supported organization creates trustworthy visibility through logging, monitoring, alerting, and security operations. Chapter 12 turns that visibility into preventive action. The focus is on maintaining approved system configurations, discovering weaknesses before they are exploited, deciding which weaknesses matter most, deploying patches and other corrections safely, and proving that the corrected state remains in place after the ticket is closed.

For many organizations, vulnerability management and patch management are treated as monthly administrative routines. A scanner runs, a report is exported, operating-system updates are pushed, and the team assumes the problem has been addressed. CMMC readiness requires a more disciplined view. The organization must know which assets are in scope, what secure state each asset is expected to maintain, how weaknesses are identified, how remediation priorities are set, who owns the corrective action, how changes are tested, and how successful implementation is verified. A report is evidence of discovery. It is not evidence of remediation.

This distinction is especially important for MSPs. Harbor Point Engineering depends on NorthStar Managed Services for endpoint administration, server support, network management, cloud configuration, remote monitoring and management, and routine patching. Beacon Security contributes threat and vulnerability intelligence. Some corrections can be executed immediately by NorthStar. Others require Harbor Point approval, application-owner testing, a maintenance window, a cloud-provider action, a vendor upgrade, or a compensating operational measure. The working model must make those dependencies visible rather than hiding them inside a service desk.

The chapter continues the Harbor Point, NorthStar, and Beacon case study. The objective is not to create a perfect environment in which no vulnerability ever appears. That is unrealistic. The objective is to create a controlled process that finds weaknesses, reduces unnecessary exposure, maintains approved configurations, responds quickly to high-risk conditions, documents justified exceptions, and produces credible evidence that the process operates throughout the year.

As of September 20, 2026, the Department has announced the suspension of CMMC Phase II implementation while Phase I self-assessment requirements remain in place. The underlying safeguarding obligations in applicable contracts remain relevant. The material in this chapter therefore emphasizes durable security operations rather than preparation for one assessment date. Organizations should always verify the current contract clauses, CMMC program guidance, and authoritative NIST sources that apply to their environment.

Learning Objectives

- Explain the relationship among configuration management, vulnerability management, patch management, change control, and CMMC evidence.
- Build an authoritative baseline for hardware, software, firmware, services, security settings, and documentation.
- Detect and investigate configuration drift across endpoints, servers, network devices, cloud resources, and security platforms.
- Design vulnerability discovery coverage that reconciles scanner results with the asset inventory and actual CUI scope.
- Prioritize remediation using exploitability, exposure, business impact, asset criticality, threat intelligence, and operational constraints rather than CVSS alone.
- Distinguish a vulnerability finding from a validated weakness, an accepted exception, a compensating mitigation, and a completed remediation.
- Plan routine and emergency patching as preventive maintenance while protecting availability and mission operations.
- Verify patch and configuration changes after deployment instead of treating tool success messages as final proof.
- Define customer, MSP, MSSP, cloud-provider, software-vendor, and application-owner responsibilities for remediation and evidence.
- Create dashboards, service levels, and management reviews that measure risk reduction instead of simply counting tickets.

Source Context and Operating Principle

NIST SP 800-171 Revision 2 remains the security-requirement baseline used by the currently published CMMC Level 2 framework discussed throughout this book. Configuration Management requirements address baseline configurations, secure settings, change control, least functionality, and restrictions on nonessential programs and services. System and Information Integrity requirements address flaw remediation, malicious-code protection, security alerts and advisories, and system monitoring. These topics converge operationally in vulnerability, configuration, and patch management.

NIST SP 800-40 Revision 4 describes enterprise patch management as preventive maintenance: identifying, prioritizing, acquiring, installing, and verifying patches, updates, and upgrades throughout the organization. NIST SP 1800-31 provides practical implementation guidance for routine and emergency patching, inventory, temporary mitigation, and protection of patch-management systems themselves. This

chapter uses those principles without turning the NIST publications into a vendor-specific recipe.

The operating principle for an MSP is simple to state but demanding to maintain: every in-scope asset should have a known owner, an expected secure state, an active method of weakness discovery, a defined remediation path, and a retrievable record of what changed. When any one of those elements is missing, the organization may have a technical control but still lack an auditable management process.

Core idea: A vulnerability scan tells the organization what may be wrong. Configuration and patch management determine what the organization does about it. Verification proves whether the correction actually worked.

12.1 Establish One Integrated Weakness-Management Program

Establish One Integrated Weakness-Management Program is a core part of program governance because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is fragmented ownership. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes policy, scope, roles, workflow, review cadence. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a

defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to turn scanner findings, drift, advisories, and patch status into one managed risk-reduction process. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

From an assessment perspective, strong implementation normally combines three kinds of proof. Examine evidence shows the approved process, current reports, tickets, exports, and configuration state. Interview evidence shows that the people performing the work understand triggers, approvals, exceptions, and escalation. Test evidence demonstrates that the technical process behaves as described: a scan reaches the intended population, a configuration change is detected, a patch is deployed to a controlled target, or a rescanning step confirms closure. No single screenshot should be asked to prove the entire control.

- Operating record: maintain current policy, scope, roles, workflow, review cadence.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.2 Start with an Authoritative Asset and Software Inventory

Start with an Authoritative Asset and Software Inventory is a core part of inventory coverage because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized

correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is unknown systems and unsupported software. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes asset register, software inventory, ownership, CUI relevance. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to make every later scan, baseline, patch, and exception traceable to a known asset. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current asset register, software inventory, ownership, CUI relevance.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.3 Classify Assets by Security and Operational Criticality

Classify Assets by Security and Operational Criticality is a core part of risk context because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is equal treatment of unequal systems. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes criticality tiers, business owner, recovery priority, exposure. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to apply remediation urgency that reflects both security consequence and mission impact. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current criticality tiers, business owner, recovery priority, exposure.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.

- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For classify assets by security and operational criticality, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.4 Define the Expected Secure State

Define the Expected Secure State is a core part of configuration intent because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is security by assumption. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes baseline documents, build standards, approved services, security settings. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to make the desired state explicit enough to test and reproduce. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current baseline documents, build standards, approved services, security settings.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.5 Separate Baseline, Standard, Procedure, and Evidence

Separate Baseline, Standard, Procedure, and Evidence is a core part of document discipline because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is confusing policy language with implementation. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes approved baseline, build procedure, configuration export, validation record. The

evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to show the difference between what should happen and what actually happened. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current approved baseline, build procedure, configuration export, validation record.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.6 Assign Customer and Provider Responsibility

Assign Customer and Provider Responsibility is a core part of shared responsibility because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is work disappearing between contracts and teams. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory.

None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes responsibility matrix, SLA, ticket ownership, escalation. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to ensure every vulnerability and configuration action has one accountable path. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current responsibility matrix, SLA, ticket ownership, escalation.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.7 Protect the Management Plane

Protect the Management Plane is a core part of administrative security because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset,

determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is compromise of RMM, patching, or configuration tools. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes MFA, privileged access, audit logs, segmentation, admin review. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to protect the systems that can change large numbers of customer devices. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current MFA, privileged access, audit logs, segmentation, admin review.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.8 Build Evidence into Normal Operations

Build Evidence into Normal Operations is a core part of evidence by design because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is assessment-week reconstruction. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes tickets, reports, exports, approvals, verification. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to produce assessment evidence as a by-product of ordinary service delivery. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current tickets, reports, exports, approvals, verification.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.

- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For build evidence into normal operations, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.9 Create Secure Baseline Configurations

Create Secure Baseline Configurations is a core part of baseline engineering because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is inconsistent builds. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes gold images, configuration profiles, benchmark mapping, approvals. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to establish repeatable settings for each supported technology class. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current gold images, configuration profiles, benchmark mapping, approvals.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.10 Use Hardening Benchmarks Carefully

Use Hardening Benchmarks Carefully is a core part of benchmark use because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is blindly applying a generic benchmark. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes tailored benchmark profile, exceptions, testing, approval. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who

approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to use recognized hardening guidance without breaking required business functions. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current tailored benchmark profile, exceptions, testing, approval.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.11 Control Administrative Configuration Changes

Control Administrative Configuration Changes is a core part of change control because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is unreviewed drift. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s

ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes change ticket, approver, implementation record, rollback plan. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to link security-sensitive changes to authorized decisions and technical evidence. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current change ticket, approver, implementation record, rollback plan.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.12 Detect Configuration Drift

Detect Configuration Drift is a core part of drift monitoring because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected

state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is silent deviation from the approved state. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes compliance scans, configuration comparison, alerts, remediation tickets. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to identify unauthorized or accidental changes before they become persistent weaknesses. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current compliance scans, configuration comparison, alerts, remediation tickets.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For detect configuration drift, ask whether the service agreement,

technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.13 Manage Local Administrator and Privileged Settings

Manage Local Administrator and Privileged Settings is a core part of privileged configuration because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is standing privilege and shared accounts. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes local admin inventory, role assignment, policy enforcement, review. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to reduce pathways that allow a configuration weakness to become system compromise. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current local admin inventory, role assignment, policy enforcement, review.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.14 Remove Unnecessary Services and Functions

Remove Unnecessary Services and Functions is a core part of least functionality because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is attack surface created by convenience. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes service inventory, disabled features, approved exceptions, validation. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to reduce exposed functionality while preserving required operations. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current service inventory, disabled features, approved exceptions, validation.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.15 Control Software Installation and Execution

Control Software Installation and Execution is a core part of software governance because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is unmanaged or unsupported applications. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes approved software list, deployment policy, application controls, exception record. The evidence does not have to live in one product, but the records must be

reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to keep software state supportable, patchable, and consistent with the system baseline. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current approved software list, deployment policy, application controls, exception record.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.16 Treat Baseline Changes as Lifecycle Events

Treat Baseline Changes as Lifecycle Events is a core part of baseline lifecycle because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is stale standards after platform change. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the

organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes revision history, architecture review, versioned baseline, communication. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to keep documented secure states aligned with technology and mission changes. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current revision history, architecture review, versioned baseline, communication.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For treat baseline changes as lifecycle events, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.17 Design Vulnerability Discovery Coverage

Design Vulnerability Discovery Coverage is a core part of scan architecture because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is blind spots mistaken for clean results. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes scanner scope, credentials, schedules, network paths, agent coverage. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to ensure the discovery method reaches every relevant technology and boundary. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current scanner scope, credentials, schedules, network paths, agent coverage.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.

- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.18 Use Authenticated Scanning Where Appropriate

Use Authenticated Scanning Where Appropriate is a core part of scan depth because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is surface-only results. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes credentialed scan configuration, protected credentials, success metrics. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to improve visibility into missing patches, local settings, and installed software. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current credentialed scan configuration, protected credentials, success metrics.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.19 Reconcile Scanner Coverage to the Asset Inventory

Reconcile Scanner Coverage to the Asset Inventory is a core part of coverage assurance because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is missing assets hidden by percentage metrics. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes asset-to-scan reconciliation, last-seen date, exclusions, investigation. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to prove that a high scan success rate actually represents the in-scope population. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current asset-to-scan reconciliation, last-seen date, exclusions, investigation.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.20 Validate Findings Before Committing Remediation

Validate Findings Before Committing Remediation is a core part of finding quality because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is false positives and duplicate work. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes technical validation, affected version, source evidence, owner. The evidence does not

have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to convert scanner output into actionable, trusted findings. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current technical validation, affected version, source evidence, owner.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For validate findings before committing remediation, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.21 Prioritize Beyond CVSS

Prioritize Beyond CVSS is a core part of risk prioritization because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is severity-only queues. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes exploitability, exposure, asset value, active exploitation, compensating controls. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to direct limited engineering effort to the weaknesses most likely to cause harm. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current exploitability, exposure, asset value, active exploitation, compensating controls.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.22 Use Threat Intelligence and Known Exploitation Data

Use Threat Intelligence and Known Exploitation Data is a core part of threat-informed remediation because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is ignoring active attacker behavior. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes vendor advisory, CISA KEV review, SOC intelligence, exposure analysis. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to increase urgency when reliable evidence shows a vulnerability is being exploited. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current vendor advisory, CISA KEV review, SOC intelligence, exposure analysis.
- Ownership: identify one accountable customer or provider role and a backup role.

- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.23 Manage Vulnerabilities in Cloud and SaaS Services

Manage Vulnerabilities in Cloud and SaaS Services is a core part of cloud weakness management because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is assuming provider ownership covers tenant configuration. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes cloud findings, tenant posture, provider notices, configuration evidence. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to separate provider infrastructure responsibility from customer tenant responsibility. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be

reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current cloud findings, tenant posture, provider notices, configuration evidence.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.24 Handle Unsupported and End-of-Life Technology

Handle Unsupported and End-of-Life Technology is a core part of technology lifecycle because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is permanent exposure from unpatchable assets. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes EOL register, replacement plan, isolation, exception approval. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a

configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to prevent legacy systems from becoming invisible long-term risk. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current EOL register, replacement plan, isolation, exception approval.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For handle unsupported and end-of-life technology, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.25 Treat Patching as Preventive Maintenance

Treat Patching as Preventive Maintenance is a core part of patch strategy because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is reactive patching only after incidents. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform

begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes patch policy, maintenance calendar, risk tiers, verification. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to make updates a normal reliability and security function rather than an emergency project. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current patch policy, maintenance calendar, risk tiers, verification.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.26 Maintain Trusted Update Sources

Maintain Trusted Update Sources is a core part of patch integrity because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The

question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is malicious or untrusted updates. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes vendor source, repository controls, signature validation, access restrictions. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to protect the supply path from vendor release to deployed package. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current vendor source, repository controls, signature validation, access restrictions.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.27 Separate Routine and Emergency Patching

Separate Routine and Emergency Patching is a core part of operating modes because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is using one slow workflow for every situation. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes standard cadence, emergency criteria, fast approval, after-action review. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to respond quickly to severe exposure without abandoning control. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current standard cadence, emergency criteria, fast approval, after-action review.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.

- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.28 Test Patches and Configuration Changes

Test Patches and Configuration Changes is a core part of predeployment assurance because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is production outages from untested change. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes test ring, pilot group, application validation, rollback. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to balance speed with operational stability. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current test ring, pilot group, application validation, rollback.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For test patches and configuration changes, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.29 Use Deployment Rings and Maintenance Windows

Use Deployment Rings and Maintenance Windows is a core part of controlled rollout because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is all-at-once failures. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes pilot, early adopter, broad deployment, exception groups. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a

vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to limit blast radius and create decision points during large-scale change. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current pilot, early adopter, broad deployment, exception groups.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.30 Coordinate Reboots, Downtime, and User Impact

Coordinate Reboots, Downtime, and User Impact is a core part of availability planning because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is technically successful but operationally disruptive remediation. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence

which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes maintenance notice, restart policy, business approval, deferred reboot tracking. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to make patch completion include the operational steps required for activation. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current maintenance notice, restart policy, business approval, deferred reboot tracking.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.31 Verify Patch Installation and Effective State

Verify Patch Installation and Effective State is a core part of post-change verification because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is false success from deployment tools. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes version check, rescanning, agent status, sample validation. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to prove the vulnerability or outdated state is actually gone. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current version check, rescanning, agent status, sample validation.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.32 Handle Failed Patches and Rollback

Handle Failed Patches and Rollback is a core part of failure recovery because vulnerability and configuration work succeeds only when the organization can

connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is stalled or partially remediated systems. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes failure queue, rollback record, root cause, retry plan. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to keep failed deployment from disappearing inside aggregate compliance percentages. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current failure queue, rollback record, root cause, retry plan.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.

- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For handle failed patches and rollback, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.33 Manage Exceptions and Temporary Mitigations

Manage Exceptions and Temporary Mitigations is a core part of exception governance because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is indefinite deferral. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes risk statement, owner, compensating action, expiration, review. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to make postponement visible, time-bound, and justified. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information

before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current risk statement, owner, compensating action, expiration, review.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.34 Integrate Vulnerability Management with the SOC

Integrate Vulnerability Management with the SOC is a core part of security operations integration because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is scanner data isolated from detection. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes shared context, alert enrichment, exploit watch, incident escalation. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and

a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to connect preventive weakness data with evidence of attacker activity. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current shared context, alert enrichment, exploit watch, incident escalation.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.35 Manage MSP Multi-Tenant Patch Operations

Manage MSP Multi-Tenant Patch Operations is a core part of multi-tenant service design because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is cross-customer errors and generic evidence. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are

protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes customer rings, tenant tags, scoped reports, approval boundaries. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to scale operations without losing customer-specific accountability. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current customer rings, tenant tags, scoped reports, approval boundaries.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.36 Control Remote Monitoring and Management Changes

Control Remote Monitoring and Management Changes is a core part of RMM governance because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is high-impact automation without safeguards. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization's ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes script approval, role controls, audit logs, test group. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to treat automation as privileged change rather than merely technician convenience. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person's memory.

- Operating record: maintain current script approval, role controls, audit logs, test group.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For control remote monitoring and management changes, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must

manually reconstruct the evidence, the service design is incomplete.

12.37 Address Network Devices and Appliances

Address Network Devices and Appliances is a core part of infrastructure patching because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is endpoint-centric programs. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes firmware inventory, vendor advisory tracking, maintenance testing, backup config. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to cover firewalls, switches, VPNs, storage, and other appliances in the same governance model. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current firmware inventory, vendor advisory tracking, maintenance testing, backup config.

- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.38 Address Containers, Images, and Ephemeral Workloads

Address Containers, Images, and Ephemeral Workloads is a core part of modern workload management because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is patching running instances without fixing source images. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes image scanning, base image ownership, rebuild pipeline, registry policy. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to remove vulnerabilities at the source so they do not reappear on redeployment. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder

to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current image scanning, base image ownership, rebuild pipeline, registry policy.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.39 Manage Specialized and Operational Technology

Manage Specialized and Operational Technology is a core part of specialized assets because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is unsafe application of general IT patch practices. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes vendor coordination, safety review, isolation, compensating controls. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and

a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to reduce risk without damaging equipment, warranty, safety, or mission operation. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person's memory.

- Operating record: maintain current vendor coordination, safety review, isolation, compensating controls.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.40 Measure Outcomes Instead of Activity

Measure Outcomes Instead of Activity is a core part of metrics because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is counting scans and tickets rather than risk reduction. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization's ability to state with confidence which

systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes coverage, age, time-to-remediate, drift, exception aging, verification. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to show whether the program is reducing exploitable exposure. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current coverage, age, time-to-remediate, drift, exception aging, verification.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For measure outcomes instead of activity, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.41 Harbor Point Case Study: Baseline Breakdown

Harbor Point Case Study: Baseline Breakdown is a core part of case-study baseline because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor

Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is inconsistent endpoint and server builds. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes baseline comparison, drift findings, ownership decisions. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to demonstrate how a small inconsistency becomes a measurable CMMC readiness issue. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current baseline comparison, drift findings, ownership decisions.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.42 Harbor Point Case Study: Critical Vulnerability Response

Harbor Point Case Study: Critical Vulnerability Response is a core part of case-study emergency because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is actively exploited weakness. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes triage, emergency change, deployment ring, rescan, evidence. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to walk through an urgent remediation from intelligence to verified closure. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current triage, emergency change, deployment ring, rescan, evidence.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.

- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.43 Harbor Point Case Study: Legacy Engineering System

Harbor Point Case Study: Legacy Engineering System is a core part of case-study exception because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is unpatchable business-critical software. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes isolation, access restriction, monitoring, replacement milestone. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to show how a temporary mitigation differs from pretending the weakness is fixed. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process,

locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current isolation, access restriction, monitoring, replacement milestone.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.44 Workshop: Build the Vulnerability-to-Closure Workflow

Workshop: Build the Vulnerability-to-Closure Workflow is a core part of workshop because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is unclear handoffs. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes workflow map, states, owners, evidence requirements. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree,

the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to turn organization-specific responsibilities into a repeatable operating model. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person's memory.

- Operating record: maintain current workflow map, states, owners, evidence requirements.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For workshop: build the vulnerability-to-closure workflow, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

12.45 Workshop: Reconcile Inventory, Scan, and Patch Data

Workshop: Reconcile Inventory, Scan, and Patch Data is a core part of workshop because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is conflicting tool populations. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins

reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes cross-system comparison, missing assets, stale agents, exception review. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to find the gaps that aggregate dashboards conceal. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current cross-system comparison, missing assets, stale agents, exception review.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.46 Field Guide for Assessment Evidence

Field Guide for Assessment Evidence is a core part of assessment evidence because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset,

determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is tool screenshots without context. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes policy, baseline, scan, ticket, approval, verification, interview. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to prepare evidence that shows both design and sustained operation. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current policy, baseline, scan, ticket, approval, verification, interview.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.47 Common Failure Patterns and Corrections

Common Failure Patterns and Corrections is a core part of failure patterns because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is recurring weak practices. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes symptom, root cause, corrective action, validation. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to help MSPs recognize why apparently mature programs still fail under examination. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current symptom, root cause, corrective action, validation.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.

- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

12.48 Sustain the Program After the Assessment

Sustain the Program After the Assessment is a core part of sustainment because vulnerability and configuration work succeeds only when the organization can connect technical state to an accountable management process. In the Harbor Point environment, the question is never only whether a tool can display a finding. The question is whether Harbor Point and NorthStar can identify the affected asset, determine the expected state, assign responsibility, make an authorized correction, verify the result, and preserve enough evidence to explain what occurred later.

The principal failure condition in this area is readiness decay. This often develops gradually. A technician makes a reasonable one-time decision, an exception is not revisited, a software version changes, or a managed-service platform begins reporting a different population than the asset inventory. None of these events necessarily creates an immediate incident. Together, however, they weaken the organization’s ability to state with confidence which systems are protected and which weaknesses remain open. That is why mature programs use both technical automation and explicit governance.

Harbor Point therefore expects NorthStar to maintain a working record that includes monthly operations, quarterly review, annual baseline refresh, change triggers. The evidence does not have to live in one product, but the records must be reconcilable. A ticket can show who approved a change, a management console can show the deployed state, a vulnerability platform can show the pre- and post-remediation condition, and a configuration repository can show the approved baseline. When those records agree, the organization has a defensible story. When they conflict, the conflict itself becomes a readiness finding that needs investigation.

The operational objective is to make vulnerability and configuration management a continuing security service. This should be designed into ordinary service delivery. The MSP should not wait for an assessor, customer executive, or incident responder to ask for the information before discovering that the records cannot be reproduced. A backup engineer should be able to follow the documented process, locate the authoritative sources, and reach the same conclusion without relying on one person’s memory.

- Operating record: maintain current monthly operations, quarterly review, annual baseline refresh, change triggers.
- Ownership: identify one accountable customer or provider role and a backup role.
- Trigger: define what event starts the workflow and what conditions increase urgency.
- Verification: require objective evidence that the desired state was achieved.
- Exception handling: document residual risk, compensating actions, expiration, and review.
- Evidence retrieval: ensure customer-specific records can be produced without exposing other tenants.

MSP checkpoint: For sustain the program after the assessment, ask whether the service agreement, technical workflow, and evidence path all describe the same responsibility. If the contract says the MSP owns the activity but the customer must manually reconstruct the evidence, the service design is incomplete.

Vulnerability Prioritization Model for MSP Operations

Severity is useful, but severity alone does not determine business urgency. Harbor Point uses a structured prioritization discussion so that a medium-severity weakness on an internet-exposed CUI gateway can receive more attention than a higher-scoring weakness on an isolated test system. The model is deliberately transparent: the purpose is to make reasoning reproducible, not to create a proprietary risk score that replaces professional judgment.

Factor	Questions	Effect on priority
Known exploitation	Is the vulnerability in an authoritative known-exploited catalog or supported by credible active-exploitation intelligence?	Substantially increases urgency.
External exposure	Is the affected service reachable from the internet, partner networks, remote access, or an untrusted segment?	Increases likelihood and urgency.
CUI/security role	Does the asset process CUI or provide security protection to CUI systems?	Increases impact and assessment significance.
Privilege required	Can exploitation yield administrative, system, or lateral-movement capability?	Increases potential impact.
Compensating controls	Are exploitation paths blocked by segmentation, application control, isolation, or other verified measures?	May reduce immediate likelihood, but does not remove the vulnerability.
Business criticality	Would remediation or exploitation significantly affect mission operations?	Shapes testing, scheduling, and executive approval.
Patch availability	Is a stable vendor fix available and supported for the installed version?	Enables direct remediation; absence may require mitigation or upgrade.
Age and recurrence	Has the weakness remained open or reappeared across multiple cycles?	Raises governance concern and may indicate process failure.

Patch Lifecycle Field Guide

Stage	Operational expectation
1. Discover	Receive vendor advisory, scanner finding, software-inventory signal, SOC intelligence, or operational notification.
2. Validate	Confirm affected product, version, asset population, exploit conditions, and whether the finding is real.
3. Prioritize	Use exploitability, exposure, asset criticality, CUI/security role, and compensating controls.
4. Decide	Select patch, upgrade, configuration mitigation, isolation, service disablement, or approved temporary exception.
5. Prepare	Obtain the update from a trusted source, define deployment ring, backup or rollback, testing, outage needs, and approvals.
6. Pilot	Deploy to a representative controlled group and validate application and security behavior.
7. Deploy	Expand according to the approved maintenance or emergency process.
8. Verify	Confirm installation, reboot or activation where required, rescan, and investigate failures.
9. Close	Attach evidence, document residual risk, update inventory or baseline if needed, and close only after verification.
10. Learn	Review failures, emergency actions, recurring exceptions, and opportunities to improve automation or service design.

CMMC-Focused Evidence Package

- Configuration-management policy and procedures that define baseline, change control, least functionality, approved software, and review responsibilities.
- Current baseline configurations for representative endpoints, servers, network devices, cloud services, and security platforms.
- Asset and software inventories showing scope, ownership, versions, and lifecycle status.

- Vulnerability-scanning architecture, schedules, credentialed-scan configuration, coverage metrics, and sample findings.
- Reconciliation showing that the scanned population matches the expected in-scope population, including documented exclusions.
- Sample remediation tickets that show finding, priority, owner, change approval, deployment evidence, verification, and closure.
- Patch-management policy, routine schedule, emergency patch criteria, test-ring design, rollback procedures, and failure queues.
- Exception records showing risk acceptance authority, compensating measures, expiration dates, and review status.
- Configuration drift reports and sample corrective actions.
- MSP/MSSP reports that are customer-specific and can be traced to provider systems without exposing other customers.
- Meeting or governance records showing management review of aging vulnerabilities, unsupported technology, exceptions, and recurring failures.
- Post-remediation scan or configuration evidence proving that selected corrections actually changed the technical state.

Chapter 12 Implementation Checklist

- Confirm the in-scope asset inventory is current and reconciled to endpoint, network, cloud, and scanner populations.
- Maintain software and firmware inventory sufficient to identify affected versions and unsupported products.
- Define approved baseline configurations for each major technology class.
- Version and approve baseline changes; keep build standards synchronized with the approved baseline.
- Protect RMM, patching, vulnerability, and configuration platforms with strong privileged-access controls and audit logging.
- Define vulnerability scan coverage, credentials, schedules, exclusions, and failure handling.
- Investigate assets that are missing, stale, unreachable, or not successfully authenticated during scans.
- Validate findings before assigning large remediation projects or closing suspected false positives.
- Prioritize with exploitability, external exposure, CUI relevance, asset criticality, threat intelligence, and compensating controls.

- Include cloud tenant configuration, SaaS administrative settings, network appliances, containers, mobile devices, and specialized assets where applicable.
- Maintain a documented routine patch cadence and a separate emergency process.
- Use trusted update sources and protect update repositories and deployment credentials.
- Test patches and significant configuration changes on representative systems where feasible.
- Use staged deployment rings and defined rollback criteria.
- Coordinate required reboots and verify that pending restarts do not leave patches inactive.
- Rescan or otherwise validate vulnerable conditions after remediation.
- Track failed deployments individually rather than hiding them in aggregate success percentages.
- Use time-limited, approved exceptions with documented compensating controls and expiration dates.
- Identify unsupported or end-of-life systems and maintain funded replacement or isolation plans.
- Review configuration drift and unauthorized change as security events, not merely technical variance.
- Connect vulnerability intelligence to SOC monitoring and incident-response priorities.
- Require customer-specific provider evidence and preserve multi-tenant separation.
- Measure exposure age, remediation time, coverage gaps, exception age, recurrence, and verification - not just scan counts.
- Review the program after emergency patches, significant outages, platform migrations, and material architecture changes.
- Keep evidence retrieval operational throughout the year so assessment readiness is a normal service outcome.

Review Questions

1. Why should vulnerability, configuration, and patch management be treated as one integrated operating program?

2. What is the difference between an asset inventory and a vulnerability scan population?

3. Why is software inventory important to remediation?

4. What does a secure baseline represent?

5. How does a baseline differ from a build procedure?

6. Why can a generic hardening benchmark require tailoring?

7. What is configuration drift, and why does it matter?

8. Why must administrative configuration changes be tied to change control?

9. How does least functionality reduce attack surface?

10. Why should security-management platforms themselves receive strong protection?

11. What additional information can authenticated vulnerability scans reveal?

12. Why must scan coverage be reconciled to the asset inventory?

13. What is the difference between a scanner finding and a validated vulnerability?

14. Why is CVSS insufficient as the sole prioritization method?

15. How should active exploitation information change remediation urgency?

16. Why does cloud vulnerability management require attention to tenant responsibility?

17. What risks are created by end-of-life systems?

18. Why does NIST describe patching as preventive maintenance?

19. What makes an update source trustworthy?

20. When should an emergency patch process differ from the routine process?

21. Why are test groups and deployment rings useful?

22. What operational issues can make a technically installed patch incomplete?

23. Why must successful patch deployment be verified independently?

24. How should failed patch deployments be handled?

25. What makes a remediation exception controlled rather than indefinite deferral?

26. How can the SOC use vulnerability information?

27. What special risks exist when an MSP patches many customers through one multi-tenant platform?

28. Why should RMM automation be treated as privileged change?

29. Why are network devices and appliances often missed by endpoint-centric patch programs?

30. How should container vulnerabilities be remediated differently from traditional server vulnerabilities?

31. Why can operational technology require alternative remediation approaches?

32. Which metrics best show whether vulnerability exposure is actually decreasing?

33. What evidence demonstrates that a configuration baseline is operating in practice?

34. What evidence demonstrates that a vulnerability was actually closed?

35. Why should exception records include an expiration date?

36. How can an MSP preserve customer-specific evidence in a shared platform?

37. What lessons should follow an emergency patch event?

38. How did Harbor Point handle the legacy engineering system without claiming it was patched?

39. What does the inventory-scan-patch reconciliation workshop reveal?

40. Why should the program continue unchanged after an assessment is complete?

Answer Guidance

Questions 1 through 10 focus on program structure and configuration management. Strong answers distinguish the expected secure state from the procedures used to create it and from the evidence showing that the state exists. They should also emphasize inventory, least functionality, controlled change, drift detection, and protection of the administrative platforms that can modify many systems at once.

Questions 11 through 17 focus on vulnerability discovery and prioritization. Strong answers explain why coverage must be measured against the real asset population, why findings require validation, and why prioritization should combine severity with exploitability, exposure, business importance, CUI/security role, and compensating

controls. End-of-life technology requires explicit lifecycle action rather than permanent exception by habit.

Questions 18 through 25 focus on patching and exceptions. Strong answers treat patching as preventive maintenance with trusted sources, testing, staged deployment, verification, and failure handling. Emergency processes can move faster but should still preserve authorization and evidence. An exception is time-limited, approved, mitigated, reviewed, and visible to management.

Questions 26 through 32 focus on MSP operations and technology diversity. Strong answers address multi-tenant separation, privileged automation, appliances, cloud systems, containers, specialized systems, and the integration between vulnerability intelligence and security monitoring. Metrics should show exposure and closure quality rather than raw activity counts.

Questions 33 through 40 focus on assessment evidence and sustainment. Strong answers combine documentation, interviews, technical proof, and customer-specific records. Closure should be demonstrated through effective-state verification, not merely ticket status. The most important indicator of maturity is that the same process works when no assessment is scheduled.

Key Terms

Baseline Configuration: A documented and approved set of specifications and security settings used as the expected state for a system or class of systems.

Configuration Drift: A change from the approved configuration state, whether authorized, accidental, or malicious.

CVSS: Common Vulnerability Scoring System, a standardized method for describing technical vulnerability severity; useful but not sufficient by itself for business prioritization.

Authenticated Scan: A vulnerability assessment performed with authorized credentials or agents that can inspect information not visible from an unauthenticated network perspective.

Known Exploited Vulnerability: A vulnerability for which authoritative information indicates exploitation in real-world activity; such information can materially increase remediation urgency.

Patch Management: The process of identifying, prioritizing, acquiring, testing, deploying, and verifying patches, updates, and upgrades.

Preventive Maintenance: The NIST framing of enterprise patching as routine work required to maintain reliable and secure technology rather than as exceptional break-fix activity.

Deployment Ring: A staged group of systems used to sequence rollout so that changes can be validated before broad deployment.

Compensating Mitigation: A temporary or alternative technical or operational measure that reduces risk when the preferred correction cannot yet be implemented; it does not automatically mean the underlying weakness is removed.

Exception: A formally approved, time-limited departure from the normal security or remediation requirement, with documented risk, ownership, mitigation, expiration, and review.

End-of-Life (EOL): A product state in which the vendor no longer provides normal support or security updates, creating increasing security and operational risk.

RMM: Remote Monitoring and Management technology used by MSPs to administer customer endpoints and systems at scale.

Remediation Verification: Objective confirmation that a corrective action changed the effective technical state and addressed the identified weakness.

Attack Surface: The collection of exposed interfaces, services, software, accounts, pathways, and functions that an attacker may attempt to abuse.

Least Functionality: The principle of enabling only the functions, ports, protocols, services, and software necessary for authorized business operation.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. Use the current edition for CMMC scope, assessment, affirmation, external-service-provider, and program requirements.

R2. National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Relevant families include Configuration Management and System and Information Integrity.

R3. National Institute of Standards and Technology. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information. Use the applicable

assessment objectives and examine, interview, and test methods for the CMMC baseline addressed in this book.

R4. National Institute of Standards and Technology. NIST SP 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology, April 2022.

R5. National Institute of Standards and Technology / National Cybersecurity Center of Excellence. NIST SP 1800-31, Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways, April 2022.

R6. Cybersecurity and Infrastructure Security Agency. Known Exploited Vulnerabilities Catalog. Use current catalog information as one input to vulnerability prioritization; verify applicability to the organization's actual technologies and exposure.

R7. DFARS 252.204-7012 and related clauses applicable to the organization's contracts. Review current contract text for safeguarding, cyber-incident reporting, preservation, cloud, and flow-down obligations.

R8. Department CMMC resources and announcements. On July 13, 2026, the Department announced suspension of Phase II requirements while maintaining Phase I self-assessment requirements. Confirm current program status before relying on implementation dates.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance. It does not replace governing regulations, contract clauses, current CMMC program guidance, legal advice, or an authorized assessment determination.

Chapter Closing

Vulnerability management is not a scanner. Configuration management is not a baseline document. Patch management is not a monthly deployment window. Each is part of the same operating discipline: knowing what the environment should look like, finding where reality differs, deciding what risk matters first, making controlled corrections, and proving that the corrected state persists.

For an MSP, this discipline has to scale without becoming generic. Automation is valuable because it allows thousands of systems to be discovered, measured, configured, and updated consistently. But CMMC accountability still exists at the customer level. Harbor Point must be able to explain its environment, NorthStar must be able to produce customer-specific evidence, and both organizations must understand the exceptions and residual risks that remain.

The practical standard is therefore not perfection. The standard is control. New vulnerabilities will be published. Software will change. Patches will fail. Business owners will sometimes defer updates. What matters is whether those events enter a governed process quickly, whether risk is visible, whether responsibility is clear, whether evidence is preserved, and whether the organization verifies the final state. When that discipline is sustained, vulnerability and patch management stop being periodic compliance chores and become part of the organization’s normal security engineering.

CMMC for MSPs

From Readiness to Certification

Chapter 13

Incident Response and Reporting

By Dr. Charles Edwards

Detailed edition • September 2026

A practical MSP-focused guide to preparing for incidents, preserving evidence, coordinating response, satisfying contractual reporting obligations, and restoring operations.

Chapter Contents

Purpose, learning objectives, and September 2026 source context

13.1–13.8 Incident-response governance, definitions, contracts, and shared responsibility

13.9–13.16 Detection, triage, severity, scoping, CUI impact, and threat context

13.17–13.24 Containment patterns for identity, endpoint, network, cloud, email, ransomware, and privileged activity

13.25–13.32 Evidence preservation, forensic readiness, DFARS rapid reporting, and report submission

13.33–13.40 Provider coordination, government follow-up, eradication, recovery, monitoring, exercises, and metrics

13.41–13.48 Harbor Point case studies, reporting and evidence workshops, field guide, common failures, and sustainment

Incident-response checklist, review questions, answer guidance, key terms, and official references

Chapter Purpose

Chapter 11 established the visibility needed to recognize suspicious activity, and Chapter 12 established the discipline needed to correct vulnerabilities and configuration weaknesses before they become incidents. Chapter 13 addresses what happens when prevention is not enough. An organization must be able to recognize a security event, decide whether it is an incident, contain the condition without destroying needed evidence, coordinate internal and external responders, meet contractual reporting obligations, recover safely, and use what it learned to improve the environment.

For an MSP-supported defense contractor, incident response is a shared operational activity but not automatically a shared legal obligation. Beacon Security Operations may be the first organization to detect a suspicious sign-in. NorthStar Managed Services may control the identity platform, endpoint tooling, firewall, and backup systems needed to contain the event. Harbor Point Engineering may nevertheless be the contractor responsible for determining whether a covered cyber incident has occurred and for making a required report under its contract. Unless the responsibility model is explicit, valuable time can be lost while each party waits for someone else to decide what to do.

This chapter therefore treats incident response as both a cybersecurity capability and a governance capability. Technical speed matters, but speed without authority, evidence discipline, communication control, or contract awareness can create a second problem after the first one. A provider can isolate a workstation yet fail to preserve relevant logs. A SOC can close an alert as resolved even though the customer never evaluated whether covered defense information was affected. A well-meaning technician can rebuild a device before forensic evidence is captured. A manager can delay escalation because the team is uncertain whether the event meets a contractual threshold.

The Harbor Point, NorthStar, and Beacon case study continues throughout the chapter. The examples emphasize a practical operating model in which detection, decision-making, containment, evidence preservation, reporting, recovery, and lessons learned are connected through documented roles and retrievable records. The goal is not to turn every help-desk ticket into a formal incident. The goal is to ensure that significant events are recognized early, evaluated consistently, and handled in a way that protects the mission, the information, and the organization’s contractual obligations.

Current CMMC implementation timing does not reduce the importance of incident response. As of September 20, 2026, the Department has suspended CMMC Phase II

implementation while Phase I self-assessment requirements remain in place. The underlying safeguarding and cyber-incident reporting obligations in applicable contracts continue to matter. An MSP should therefore build incident response as a durable operating capability rather than as an assessment-week demonstration.

Learning Objectives

- Explain the difference among an operational event, a security event, a cybersecurity incident, and a contractually reportable cyber incident.
- Build an incident-response plan that identifies authority, escalation, contacts, providers, evidence sources, communication channels, and decision points.
- Integrate SOC alerts, user reports, identity telemetry, endpoint detections, network signals, cloud events, vulnerability context, and business impact into triage.
- Classify severity and scope without allowing a provider ticket priority to substitute for the contractor's incident determination.
- Contain identity, endpoint, network, cloud, email, ransomware, and privileged-access incidents while protecting operational continuity and evidence.
- Preserve system images, monitoring data, packet captures, malware samples, investigation notes, and chain-of-custody information when required.
- Understand the DFARS 252.204-7012 rapid-reporting timeline, media-preservation requirement, malware-submission obligation, and government follow-up provisions when that clause applies.
- Coordinate customer, MSP, MSSP, cloud-provider, legal, communications, management, subcontractor, and government roles without creating shared-responsibility ambiguity.
- Recover systems through controlled eradication, restoration, validation, enhanced monitoring, and return-to-service decisions.
- Test incident-response capability through tabletop and operational exercises, then use lessons learned and metrics to improve the program.

Source Context and Operating Principle

The CMMC Level 2 framework currently referenced in 32 CFR Part 170 uses the NIST SP 800-171 Revision 2 security-requirement baseline. Its Incident Response family requires organizations to establish an operational incident-handling capability, track and report incidents to appropriate internal and external authorities, and test the incident-response capability. NIST SP 800-171A provides the corresponding assessment objectives and examine, interview, and test methods used to evaluate those requirements. This chapter uses those sources for CMMC-oriented readiness and evidence discussions.

For general incident-response practice, NIST SP 800-61 Revision 3, finalized in April 2025, integrates incident response across cybersecurity risk management and the NIST Cybersecurity Framework 2.0. It superseded Revision 2. The publication is useful for modern response planning, but it does not replace the contractor's actual clauses, reporting instructions, or CMMC requirement source. The book therefore distinguishes operational best practice from contractually binding requirements.

When DFARS 252.204-7012 applies, the contractor must rapidly report covered cyber incidents to DoD. The clause defines rapidly report as within 72 hours of discovery, requires preservation and protection of images of known affected systems and relevant monitoring or packet-capture data for at least 90 days from submission of the report, addresses malicious-software submission, and requires access to additional information or equipment when DoD requests it for forensic analysis. These duties should be mapped before an incident occurs rather than discovered during a crisis.

The operating principle for an MSP is straightforward: detection can be delegated, technical response can be shared, and many tools can be provider-operated, but accountability must remain traceable. The customer and provider must know who can declare an incident, who can authorize disruptive containment, who preserves evidence, who contacts legal counsel, who determines contractual applicability, who submits reports, who communicates with the government, and who verifies recovery.

Operational Rule

Do not use a severity label, SOC disposition, insurance threshold, or generic incident category as a substitute for reading the customer's actual contract and determining whether the event triggers a specific reporting obligation.

13.1 Treat Incident Response as a Standing Business Capability

Incident response works only when governance is established before urgency arrives.

For an MSP-supported organization, the practical challenge is that a response plan exists only as a compliance document and is not integrated into normal operations. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point places incident response under the same governance forum that reviews CMMC scope, major changes, vulnerabilities, and provider performance. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include approved plan, named incident commander, role matrix, contact roster, exercise schedule. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

Assessment readiness is stronger when the organization can demonstrate the process using a real completed case or a controlled exercise. Examine evidence can show plans, tickets, logs, reports, approvals, and after-action records. Interviews can confirm that participants understand their responsibilities and escalation triggers. Tests can demonstrate that contacts, alternate communications, evidence retrieval, reporting access, and selected technical actions actually work. The objective is sustained capability, not a scripted performance for an assessor.

Management should also define the failure response for the process itself. If a primary contact is unavailable, a log source is missing, a provider cannot deliver evidence, a containment action fails, or a reporting portal is inaccessible, the team should know the backup path. Incident response becomes resilient when the organization has planned not only the ideal workflow but also the predictable points at which that workflow can break.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.2 Define Event, Security Event, Incident, and Reportable Incident

Language shapes action during an incident, so definitions must support consistent decisions.

For an MSP-supported organization, the practical challenge is that teams use the word incident for every alert or, at the other extreme, reserve it only for confirmed data theft. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon may label an alert high severity, but Harbor Point separately determines whether the facts constitute a cybersecurity incident and whether a reporting clause applies. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include definitions, triage criteria, decision log, escalation thresholds. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.3 Establish Incident Authority and Decision Rights

Authority must be visible before responders are forced to choose between speed and approval.

For an MSP-supported organization, the practical challenge is that responders know technical actions but not who can authorize containment, shutdown, external notification, or return to service. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between

technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar can isolate a workstation under a preapproved runbook, while broader network shutdown requires Harbor Point authorization unless emergency authority is invoked. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include RACI, emergency authority matrix, executive delegation, after-hours contacts. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.4 Build the Incident-Response Plan Around Real Workflows

A plan becomes useful when it mirrors the systems, people, providers, and decisions used in real operations.

For an MSP-supported organization, the practical challenge is that the plan describes abstract phases but not the actual systems, providers, tools, locations, or escalation paths used by the organization. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point maps identity, endpoint, firewall, email, backup, ticketing, SIEM, and cloud responsibilities into the plan so responders do not improvise ownership. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include incident plan, provider runbooks, system maps, contact methods, recovery dependencies. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.5 Maintain an Incident Contact and Escalation Matrix

Communication failure can turn a manageable incident into an organizational crisis.

For an MSP-supported organization, the practical challenge is that contact lists are stale, single-threaded, or unavailable when primary systems are affected. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar and Beacon maintain tested after-hours paths that do not depend on Harbor Point email if the email tenant is part of the incident. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include primary and backup contacts, out-of-band channels, legal and executive contacts, provider escalation numbers. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.6 Map Contractual and Regulatory Reporting Duties Before an Incident

Contract obligations should be converted into operational decision points before an incident occurs.

For an MSP-supported organization, the practical challenge is that the response team begins reading contract clauses only after a serious event is underway. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point records which contracts contain DFARS 252.204-7012 and which business owner and counsel support the reporting decision. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include contract matrix, clause inventory, reporting portals, certificate prerequisites, subcontractor flow-down map. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should

be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

Contract and Reporting Note

Contract reporting requirements are not universal. Build the matrix from the clauses and reporting instructions that actually apply to each contract and subcontract.

13.7 Define Customer, MSP, MSSP, CSP, and Subcontractor Responsibilities

Shared service delivery requires explicit incident ownership at every boundary.

For an MSP-supported organization, the practical challenge is that every provider assumes another party will preserve evidence or make the external report. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon owns first-line detection, NorthStar owns technical containment for managed systems, and Harbor Point owns contract-level incident determination and reporting. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include customer responsibility matrix, incident annex, service-level targets, evidence-delivery commitments. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence

contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.8 Protect Incident Communications and Alternate Channels

Incident communications must remain trustworthy even when normal enterprise services are suspect.

For an MSP-supported organization, the practical challenge is that the compromised collaboration platform becomes the sole place where responders discuss the incident. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point predefines an emergency collaboration channel and telephone bridge for incidents affecting its primary identity or messaging environment. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include alternate communications plan, access restrictions, secure conference process, distribution rules. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.

- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.9 Build Detection Coverage from the Environment, Not the Tool

Detection should be engineered from the environment and threat pathways rather than from the capabilities of one product.

For an MSP-supported organization, the practical challenge is that the organization equates having a SIEM or EDR license with complete incident visibility. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon reconciles monitored sources with Harbor Point’s asset and CUI-scope inventories so that systems missing telemetry are treated as coverage gaps. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include log-source inventory, detection coverage map, unsupported asset list, monitoring ownership. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.10 Connect Logging and Alerting to Incident Triage

A security alert becomes operationally useful only when it enters a governed triage and escalation process.

For an MSP-supported organization, the practical challenge is that alerts remain isolated in provider consoles and never enter a customer-visible incident workflow. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

A suspicious sign-in creates both a SOC case and a customer incident record with cross-referenced identifiers rather than two disconnected histories. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include alert-to-ticket mapping, case identifiers, timestamps, escalation records, disposition evidence. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.11 Make User Reporting a Formal Detection Source

Employees and administrators are important sensors because they notice context that automated tools may not see.

For an MSP-supported organization, the practical challenge is that employees report suspicious behavior informally and the evidence disappears into chat or voicemail.

This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

A Harbor Point engineer who notices an unexpected MFA prompt can report it through a defined process that immediately routes the event to Beacon and NorthStar. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include reporting channel, intake form, help-desk category, awareness records, escalation timer. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.12 Triage for Facts Before Reaching Conclusions

Early triage should maximize factual clarity while minimizing assumptions.

For an MSP-supported organization, the practical challenge is that responders close alerts based on one benign explanation before checking correlated identity, endpoint, network, and business context. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon checks whether a suspicious login coincides with impossible travel, endpoint activity, mailbox changes, VPN access, or privileged actions before disposition. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include triage worksheet, correlated evidence, analyst notes, decision timestamps. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.13 Use Severity to Drive Response, Not to Replace Judgment

Severity is a coordination tool, not a substitute for technical or contractual judgment.

For an MSP-supported organization, the practical challenge is that ticket priority is mistaken for incident significance or contractual reportability. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

A low-volume identity compromise on an administrator may receive greater response priority than a noisy malware alert on an isolated test device. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include severity matrix, business impact criteria, escalation timing, executive notification rules. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.14 Establish and Revisit Incident Scope

Incident scope is a living hypothesis that must be revised as evidence develops.

For an MSP-supported organization, the practical challenge is that teams freeze their initial scope and fail to expand the investigation as new evidence appears. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar begins with one endpoint but expands the scope when shared credentials and remote-management activity indicate possible lateral access. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include affected asset list, identity list, time window, data-flow map, scope-change log. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.15 Evaluate CUI, CDI, and Operationally Critical Support Impact

Technical impact and information impact are related but not identical questions.

For an MSP-supported organization, the practical challenge is that technical containment succeeds but no one determines what protected information or contract work may have been affected. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point traces the incident through engineering file stores, email, remote support, backups, and collaboration services rather than assuming the affected laptop was the full scope. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include information-impact assessment, data locations, access history, contract linkage, management decision. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.

- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

Contract and Reporting Note

Do not assume that because a device contained CUI at some point, every security event involving that device is automatically a reportable cyber incident. Determine the facts, contract applicability, and actual compromise conditions.

13.16 Use Threat Intelligence as Context, Not as Proof

Threat intelligence adds context, but observed evidence remains the foundation for the organization’s decisions.

For an MSP-supported organization, the practical challenge is that a known indicator or vendor advisory is treated as definitive attribution or as proof that every system is compromised. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon uses threat intelligence to prioritize searches and containment while clearly distinguishing observed facts from external reporting. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include indicator sources, confidence notes, matching results, intelligence timestamps. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.

- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.17 Select Containment Actions Deliberately

Containment is a risk decision that balances stopping harm, preserving evidence, and protecting mission operations.

For an MSP-supported organization, the practical challenge is that the fastest technical action destroys evidence, creates unnecessary outage, or pushes an attacker into a different channel. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point and NorthStar choose whether to isolate, disable, block, rotate, segment, or monitor based on risk, evidence needs, and mission impact. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include containment decision log, approvals, rollback plan, evidence-preservation steps. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.

- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.18 Respond to Identity and Credential Compromise

Identity compromise requires response to credentials, sessions, tokens, roles, and trust relationships, not just passwords.

For an MSP-supported organization, the practical challenge is that teams reset a password but ignore tokens, sessions, MFA methods, application secrets, delegated access, and privileged roles. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar disables risky sessions, rotates affected secrets, reviews MFA registration, and checks privileged changes before restoring normal access. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include account timeline, token revocation, session termination, credential rotation, access review. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.19 Respond to Endpoint Malware and EDR Detections

Endpoint containment should preserve the evidence needed to understand what happened before the system is rebuilt.

For an MSP-supported organization, the practical challenge is that EDR quarantine is treated as complete incident closure without checking persistence, lateral movement, or data access. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon preserves relevant telemetry before NorthStar reimages an endpoint and verifies that adjacent systems show no related activity. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include EDR case, process tree, isolation record, forensic capture, reimage or remediation decision. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.20 Respond to Network and Remote-Access Compromise

Network containment must consider every path by which an adversary or compromised account could continue access.

For an MSP-supported organization, the practical challenge is that responders block one source address but fail to review VPN, firewall, remote-management, segmentation, and administrative paths. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar correlates remote access, firewall, and identity records to determine whether a compromised account reached CUI systems. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include firewall changes, VPN logs, remote-access records, network captures, segmentation validation. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.21 Respond to Cloud and SaaS Incidents

Cloud incidents require close attention to the shared-responsibility boundary and to provider-specific evidence.

For an MSP-supported organization, the practical challenge is that the organization assumes the provider owns the incident because the affected service is hosted. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that

decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point maintains customer-side responsibility for tenant configuration, user actions, reporting decisions, and evidence retrieval even when the infrastructure provider investigates platform issues. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include tenant audit logs, provider notices, configuration snapshots, identity events, support case. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.22 Respond to Email, Phishing, and Business Email Compromise

Email compromise often extends beyond the malicious message into identity, authorization, and business processes.

For an MSP-supported organization, the practical challenge is that removal of the malicious message ends the response while forwarding rules, OAuth grants, sessions, and downstream communications remain unchecked. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon searches for related messages while NorthStar revokes sessions and Harbor Point evaluates whether sensitive information was exposed or fraudulent instructions were sent. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include message trace, mailbox rules, OAuth grants, sign-in history, recipient list. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.23 Respond to Ransomware and Extortion

Ransomware compresses decision time and therefore exposes weaknesses in authority, backups, evidence, communications, and recovery planning.

For an MSP-supported organization, the practical challenge is that pressure to restore quickly leads to premature rebuilding, incomplete scoping, or destruction of evidence. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point separates business-continuity decisions from evidence preservation and validates backup integrity before restoration. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information

were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include isolation timeline, backup status, extortion communications record, forensic captures, recovery decision log. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.24 Respond to Insider and Privileged-Administrator Activity

Privileged-account incidents require restricted handling because the suspected activity may involve people who normally administer the evidence sources.

For an MSP-supported organization, the practical challenge is that the team treats suspicious administrator actions as ordinary support work or alerts the subject before evidence is secured. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar escalates anomalous privileged actions through a restricted path because the normal support team may include the account under review. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include privileged audit logs, HR/legal coordination, access review, evidence preservation record. These records should be

created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.25 Establish Forensic Readiness Before the Incident

Forensic readiness is the ability to collect and preserve useful evidence without inventing the process during a crisis.

For an MSP-supported organization, the practical challenge is that logs, images, tooling, retention, and legal authority are unavailable when investigators need them. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point identifies in advance which evidence can be collected from endpoints, cloud services, firewalls, identity systems, and provider platforms. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include forensic readiness plan, retention settings, collection tools, legal process, provider commitments. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.26 Preserve Evidence with Traceability

Evidence must remain attributable, protected, and understandable to people who were not present when it was collected.

For an MSP-supported organization, the practical challenge is that screenshots and exports are copied into ad hoc folders without source, time, collector, or integrity context. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar records who collected each artifact, from which customer tenant, using what query or method, and where the protected original is stored. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include evidence register, collector identity, timestamps, hashes where appropriate, protected repository. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.

- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.27 Preserve System Images, Monitoring Data, and Packet Captures

Preservation obligations can outlast ordinary operational log retention and therefore need explicit triggers.

For an MSP-supported organization, the practical challenge is that systems are rebuilt or logs age out before the contractual preservation window is recognized. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

When DFARS 252.204-7012 applies, Harbor Point and NorthStar preserve the required affected-system images and relevant monitoring or packet-capture data for at least 90 days from report submission. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include system images, packet captures, monitoring exports, preservation notice, retention verification. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

Contract and Reporting Note

For DFARS 252.204-7012 incidents, the clause requires preservation and protection

of images of known affected systems and relevant monitoring or packet-capture data for at least 90 days from submission of the cyber-incident report.

13.28 Handle Malicious Software Carefully

Malware evidence requires controlled handling because the artifact is both technically hazardous and potentially subject to reporting instructions.

For an MSP-supported organization, the practical challenge is that malware samples are emailed, casually copied, or sent to the wrong party. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

If malicious software is discovered and isolated in connection with a reportable incident, the team follows the applicable DoD/DC3 submission instructions rather than sending it to the contracting officer. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include sample identifier, secure storage, analysis record, submission instructions, access log. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.29 Build an Incident Timeline that Can Survive Review

A reliable timeline turns disconnected alerts and actions into an explainable incident history.

For an MSP-supported organization, the practical challenge is that the final chronology is created from memory days later and omits provider actions or time-zone differences. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon, NorthStar, and Harbor Point contribute to one synchronized timeline that distinguishes observed events from later conclusions. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include normalized timeline, source references, time-zone convention, decision entries, corrections log. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.30 Control Legal, Executive, Customer, and Public Communications

Different audiences need different information, and technical responders should not carry every communication responsibility.

For an MSP-supported organization, the practical challenge is that technical responders make external statements before facts, privilege, contract obligations, or customer commitments are understood. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point keeps operational containment moving while designated leaders and counsel control external notifications and statements. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include communication approvals, legal review path, executive brief, stakeholder matrix. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.31 Execute DFARS Rapid Reporting When the Clause Applies

Rapid reporting depends on early recognition, decision authority, and prebuilt reporting procedures.

For an MSP-supported organization, the practical challenge is that the organization waits for a perfect forensic conclusion and misses the contractual reporting window. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to

explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

DFARS 252.204-7012 defines rapidly report as within 72 hours of discovery of a cyber incident; Harbor Point's process is designed to submit known facts and continue the investigation rather than waiting for certainty. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include discovery timestamp, report decision, submission confirmation, report identifier, follow-up task list. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

Contract and Reporting Note

DFARS 252.204-7012 defines rapidly report as within 72 hours of discovery of any cyber incident when the clause applies. The response team should not treat 72 hours as a target for starting analysis.

13.32 Prepare the Cyber-Incident Report and Reporting Access in Advance

Reporting access and data collection are capabilities that should be tested before they are needed.

For an MSP-supported organization, the practical challenge is that the team discovers during the incident that required portal access, certificates, or report data are

unavailable. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point verifies reporting access and maintains a controlled worksheet so the team can assemble the required incident information without exposing passwords or unnecessary data. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include portal readiness, approved credentials, reporting worksheet, required data fields, submission receipt. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

Contract and Reporting Note

Reporting credentials, portal access, and required organizational information should be verified before an incident. Do not share reporting credentials informally or wait for a serious event to discover access problems.

13.33 Coordinate Subcontractor and Provider Incident Reporting

The prime contractor’s timeline can be affected by how quickly a subcontractor or provider recognizes and escalates an event.

For an MSP-supported organization, the practical challenge is that subcontractors or service providers notify slowly, use incompatible definitions, or assume the prime contractor will discover the incident elsewhere. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point requires NorthStar and relevant subcontractors to notify it quickly enough for Harbor Point to meet its own reporting obligations. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include flow-down clauses, notification SLAs, provider escalation path, report-content requirements. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.34 Support Government Requests for Additional Information or Equipment

A submitted report may begin a continuing information and forensic support process rather than ending the matter.

For an MSP-supported organization, the practical challenge is that the team treats report submission as the end of the obligation and is unprepared for follow-up requests. This failure usually develops at a boundary: between a SOC case and a

help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point assigns a custodian and coordination path for additional information or equipment that DoD may request for forensic analysis under the applicable clause. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include request log, evidence custodian, secure transfer process, legal coordination, equipment-access plan. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.35 Eradicate the Cause, Not Only the Symptom

Eradication should remove persistence and correct the condition that enabled the incident.

For an MSP-supported organization, the practical challenge is that responders remove malware or reset one account without correcting the exploited weakness, persistence, or insecure configuration. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar links incident eradication to the Chapter 12 vulnerability and configuration process so the weakness is corrected across every affected system. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include root-cause record, persistence checks, remediation tickets, vulnerability linkage, validation evidence. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.36 Recover Through Controlled Return to Service

Recovery should restore mission capability without recreating the compromise or hiding unresolved risk.

For an MSP-supported organization, the practical challenge is that business pressure causes systems to return before security controls, evidence needs, or monitoring are ready. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point restores services in prioritized waves and requires security checks before each wave returns to normal operation. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include recovery plan, restoration approvals, security validation, business owner acceptance, rollback criteria. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.37 Restore from Backups Without Reintroducing the Incident

Backup restoration is a security action as well as a continuity action.

For an MSP-supported organization, the practical challenge is that the organization assumes any successful backup is clean and restores compromised configurations or credentials. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

NorthStar selects recovery points using the incident timeline and validates restored systems before reconnecting them to production networks. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include backup selection rationale, integrity check, malware scan, credential reset, restore validation. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence

contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.38 Apply Enhanced Monitoring After Recovery

Recovery confidence increases when the organization actively looks for recurrence or missed persistence.

For an MSP-supported organization, the practical challenge is that the incident is closed immediately after restoration and recurring indicators are missed. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Beacon increases attention to related identities, indicators, endpoints, and network paths until Harbor Point approves a return to normal monitoring. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include heightened monitoring plan, detection changes, watch period, exit criteria, findings log. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.

- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.39 Conduct Lessons Learned as a Control Improvement Process

Lessons learned are valuable only when they become owned changes to technology, process, training, or contracts.

For an MSP-supported organization, the practical challenge is that the meeting becomes a blame session or produces observations without owners and deadlines. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Harbor Point converts lessons into changes to logging, baselines, access, training, provider contracts, and exercises rather than filing a narrative and moving on. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include after-action report, corrective actions, owners, due dates, policy and runbook changes. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.40 Measure Incident-Response Performance Carefully

Incident-response metrics should reveal bottlenecks and risk rather than reward superficial speed.

For an MSP-supported organization, the practical challenge is that leaders focus on one speed metric and reward premature closure or low incident counts. This failure usually develops at a boundary: between a SOC case and a help-desk ticket, between a provider and a customer, between technical containment and contract review, or between a fast operational decision and the evidence needed to explain that decision later. The response process should therefore define the boundary explicitly instead of assuming that the right person will recognize it under pressure.

Management reviews trends with context and distinguishes operational measures from CMMC assessment determinations or contractual compliance conclusions. The important point is not the specific product or workflow. The important point is that the customer can identify who made the decision, what facts were available at the time, which systems or information were affected, and what action followed. That traceability allows the organization to move quickly while preserving accountability.

The working record for this activity should include detection-to-triage time, escalation time, containment time, evidence completeness, repeat-incident rate, exercise findings. These records should be created as part of normal response work rather than assembled after the incident from memory. Where provider systems are involved, the records should be customer-specific and exportable without exposing other tenants. Where evidence contains CUI, credentials, personal information, threat indicators, or sensitive investigative details, access and transfer should be restricted appropriately.

- Operating proof: preserve the records produced by the normal workflow rather than creating substitute evidence later.
- Ownership proof: identify the accountable customer role, supporting provider role, and backup contact.
- Decision proof: record the facts, timestamp, authority, and rationale for significant escalation or containment actions.
- Sustainment proof: test the process periodically and update it after exercises, incidents, platform changes, and contract changes.

13.41 Harbor Point Case Study: From SOC Alert to Declared Incident

At 6:42 a.m. on a Tuesday, Beacon receives a high-confidence alert for a successful sign-in to a Harbor Point engineering account from an unusual location followed by creation of a new mailbox rule. The account normally uses a managed laptop and

multifactor authentication. Beacon opens a SOC case and begins triage. Under the service agreement, Beacon can investigate and can ask NorthStar to revoke sessions, but Beacon cannot independently declare a contractually reportable incident for Harbor Point.

Beacon correlates the sign-in with identity logs, mailbox activity, endpoint telemetry, and VPN records. The managed laptop appears healthy and was offline during the suspicious sign-in. The attacker created an inbox rule and accessed several message threads containing project references. Beacon escalates the case to NorthStar and Harbor Point under the incident matrix. NorthStar revokes sessions, disables the account temporarily, captures identity and mailbox logs, and checks for additional accounts showing the same indicators.

Harbor Point appoints its incident commander and begins the incident decision log. The team distinguishes three questions. First, is the account compromise a cybersecurity incident? Second, what systems and information were affected? Third, does any contract clause require external reporting? Counsel and the contract owner review the applicable agreements while technical responders continue containment and evidence preservation. The contractual review does not stop the investigation, and the investigation does not wait for a final reporting decision before preserving evidence.

The investigation shows that the compromised mailbox contained messages with links to CUI stored in an approved repository, but the available evidence does not show that the attacker successfully accessed the repository. Harbor Point records that distinction. It continues searching identity and repository audit logs rather than assuming that email compromise equals CUI exfiltration or, conversely, assuming that the absence of a file download ends the inquiry.

The case demonstrates why incident response must integrate detection, identity, information flow, contract review, evidence, and management authority. Beacon’s alert was necessary but not sufficient. NorthStar’s containment was necessary but not sufficient. Harbor Point’s business and contractual decision-making was necessary but could not replace technical facts. The response became reliable because the three organizations used one documented operating model.

Time	Owner	Action	Evidence/Decision
06:42	Beacon	High-confidence sign-in and mailbox-rule alert	SOC case and identity alert

Time	Owner	Action	Evidence/Decision
06:49	Beacon	Correlates sign-in, mailbox, endpoint, and VPN activity	Triage notes and query results
07:03	NorthStar	Revokes sessions and temporarily disables account	Identity administration logs
07:11	Harbor Point	Declares internal incident and activates incident team	Incident decision log
07:25	NorthStar	Preserves identity and mailbox audit data	Evidence register
07:40	Harbor Point	Begins contract and information-impact review	Contract matrix and impact worksheet

13.42 Harbor Point Case Study: Identity Compromise with CUI Repository Access

A second scenario begins with the same type of identity compromise but reaches a different conclusion because the evidence shows that the attacker used the stolen session to access Harbor Point’s CUI repository. The lesson is that incident categories are not determined by the alert name. They are determined by the facts that emerge from the investigation.

NorthStar preserves the repository audit logs and identity records before disabling additional pathways that could invalidate active sessions. Beacon searches for related indicators across other accounts. Harbor Point identifies the affected contracts, reviews which information was available to the compromised identity, and documents what the current evidence establishes and what remains unknown.

Where DFARS 252.204-7012 applies, Harbor Point’s reporting process starts from the discovery timestamp and does not wait for the investigation to become perfect. The organization prepares the required report using known facts, records assumptions and open questions internally, preserves required media and monitoring information, and continues the investigation after submission. The incident commander tracks follow-up actions so that report submission does not become the point at which technical work loses urgency.

The response also demonstrates why provider contracts should address evidence delivery. If the cloud or managed-service provider can supply customer-specific logs only after a multi-day support process, the customer may face avoidable delay. Harbor Point's service design therefore treats incident evidence latency as a security requirement, not merely as a support convenience.

13.43 NorthStar Case Study: Multi-Tenant Provider Incident Without Cross-Customer Exposure

NorthStar discovers suspicious administrative activity in its remote-management platform. Because the platform serves many customers, the first priority is to establish whether the activity is confined to NorthStar's internal administration layer or whether any customer tenant or endpoint was accessed. A provider incident can create risk for customers even when no customer evidence initially shows compromise.

NorthStar activates its provider incident plan, restricts the investigation to a need-to-know team, preserves platform logs, rotates privileged credentials, and validates administrative paths. It creates customer-specific impact records rather than sending the same generic conclusion to every customer. Harbor Point receives a notice describing what NorthStar knows, what it does not yet know, what customer systems were checked, what evidence is available, and when the next update will occur.

The case illustrates a critical MSP principle: a provider should not expose one customer's data while trying to prove another customer was unaffected. Evidence production must be tenant-aware. At the same time, the provider cannot hide behind multi-tenancy as a reason for giving customers no meaningful assurance. Contract design, logging architecture, and evidence export should make customer-specific incident support possible.

13.44 Workshop: Build the Contractual Reporting Decision Worksheet

Use this workshop to create a decision aid for each contract rather than a universal reporting checklist. The worksheet should help the incident commander and contract owner find the controlling clause, identify the reporting trigger, confirm the submission method, identify time limits, and record supporting counsel or management review. It should not attempt to predetermine every legal conclusion.

Worksheet Element	Questions to Answer
Contract/Task Order	Which agreement is affected, and what work or information does it cover?

Worksheet Element	Questions to Answer
Clause	Is DFARS 252.204-7012 or another cyber-reporting clause incorporated?
Discovery Time	When did the organization discover the cyber incident for purposes of the applicable clause?
Affected Systems	Which covered systems or provider services are known or suspected to be involved?
Information Impact	What covered defense information, CUI, or operationally critical support may be affected?
Submission Access	Who can access the required reporting portal and approved credentials?
Preservation	What systems, images, logs, monitoring data, packet captures, and samples must be preserved?
Follow-Up	Who owns government requests, updates, and continuing investigation tasks?

13.45 Workshop: Design the Evidence-Preservation Package

The objective is to define what will be collected, who will collect it, where it will be stored, and how the team will preserve attribution. The package should be appropriate to the incident; not every event requires a full disk image. The process should nevertheless make it difficult to lose critical records through ordinary retention, reimaging, log rollover, or provider platform limits.

- Create an evidence register with artifact identifier, source system, customer/tenant, collector, collection time, method, storage location, and access restrictions.
- Normalize timestamps and record the source time zone when systems use different time references.
- Preserve original exports and images separately from analyst working copies and annotations.
- Document query parameters, filters, and time windows for cloud and SIEM exports so another reviewer can understand what was included and excluded.
- Use hashes or other integrity checks when appropriate to the evidence type and investigative purpose.
- Record any evidence that could not be obtained, why it was unavailable, and what alternate sources were used.

13.46 Workshop: Run a Tabletop Exercise that Tests the Provider Boundary

A useful tabletop exercise should force participants to make decisions, not simply read the response plan aloud. Harbor Point uses a scenario in which Beacon detects suspicious remote-management activity at 8:15 p.m. on a Friday, NorthStar's primary incident manager is unavailable, Harbor Point email is considered untrusted, and one potentially affected system supports a time-sensitive defense deliverable.

The facilitator injects new facts in stages: evidence of a privileged sign-in, uncertainty about whether CUI was accessed, a failed attempt to contact one executive, a provider log source with only seven days of retention, and a question about whether an applicable DFARS clause requires reporting. Participants must demonstrate the alternate communication path, identify authority for isolation, preserve evidence, engage contract review, and maintain the incident timeline.

The exercise should end with corrective actions rather than a pass/fail score. Examples include adding a backup incident commander, increasing retention, preauthorizing selected containment actions, updating portal access, clarifying provider notification timing, and improving evidence exports. The organization then tracks those actions through the same remediation discipline used elsewhere in the CMMC program.

13.47 Incident-Response Field Guide and Common Failure Patterns

Failure Pattern	Why It Matters	Corrective Direction
SOC closes alert without customer incident review	Provider disposition may not address contract or CUI impact	Require escalation criteria and customer decision record
Password reset only	Sessions, tokens, MFA methods, rules, and delegated access may persist	Use a complete identity-containment runbook
Reimage before preservation	Can destroy evidence and make scoping harder	Preserve needed evidence before destructive remediation
No alternate communications	Primary identity/email compromise can disable coordination	Maintain and test out-of-band channels
72-hour rule treated as investigation deadline	Reporting may be delayed while team seeks certainty	Start reporting decision and evidence preservation immediately
Generic MSP incident notice	Does not establish customer-specific impact	Provide tenant-specific findings, evidence, and limitations
Report submitted, case effectively	Government follow-up and	Track post-report actions and

Failure Pattern	Why It Matters	Corrective Direction
closed	technical remediation may remain	continuing investigation
Lessons learned without owners	Same weakness reappears	Convert findings to assigned corrective actions with dates

A mature organization does not try to eliminate every incident. It tries to reduce preventable incidents, recognize meaningful events quickly, limit damage, preserve trustworthy evidence, fulfill obligations, and improve after each event. That is a more realistic and more defensible operating standard than claiming that good security means nothing will ever go wrong.

13.48 Sustain Incident Readiness Between Assessments

Incident readiness should not rise and fall with the assessment calendar. Contact lists change, provider platforms change, logging retention changes, contracts are awarded, employees leave, cloud services are added, and response tooling is replaced. Each of those changes can make a previously valid incident plan inaccurate.

Harbor Point therefore includes incident-response review in recurring governance. NorthStar verifies runbooks, technical authority, evidence sources, backup restoration dependencies, and provider escalation routes. Beacon reviews detection coverage and escalation criteria. Contract owners review new clauses and reporting pathways. Management receives concise metrics and unresolved corrective actions.

The final readiness test is simple: could the organization handle a serious event tonight using the people, tools, access, evidence, and authority that exist now? If the answer depends on one employee, an untested portal account, a provider promise that has never been exercised, or logs that may already have rolled off, the response capability is not yet mature. Sustained readiness means those dependencies are visible and actively managed.

Incident-Response Checklist for MSP-Supported Organizations

- Approve an incident-response plan that reflects the actual CUI environment, service providers, systems, and business operations.
- Define event, security event, cybersecurity incident, severity levels, and escalation criteria.
- Identify primary and backup incident commanders and the authority for disruptive containment actions.
- Maintain current customer, MSP, MSSP, CSP, legal, executive, contract, insurance, and government-reporting contacts as applicable.

- Test alternate communications that do not depend on the primary identity or email environment.
- Map cyber-reporting clauses and submission requirements by contract and subcontract.
- Verify required reporting-portal access and approved credentials before an incident.
- Define provider notification SLAs that allow the contractor to meet its own obligations.
- Reconcile monitoring coverage to the in-scope asset and service inventory.
- Route significant SOC alerts and user reports into one traceable customer incident workflow.
- Record discovery time, escalation time, decisions, containment actions, and evidence sources.
- Define identity, endpoint, network, cloud, email, ransomware, and privileged-activity runbooks.
- Preserve needed evidence before reimaging, deletion, credential changes, or other destructive actions when practicable.
- Maintain an evidence register and protected repository with customer-specific attribution.
- When DFARS 252.204-7012 applies, preserve required system images and relevant monitoring/packet-capture data for at least 90 days from report submission.
- Follow applicable instructions for malicious-software submission rather than sending samples through ordinary communication channels.
- Prepare to support government requests for additional information or equipment when required.
- Link eradication work to vulnerability, patch, configuration, and identity-remediation processes.
- Validate backups and recovery points before restoration.
- Apply heightened monitoring and defined exit criteria after recovery.
- Run tabletop exercises that include provider outages, after-hours escalation, CUI-impact uncertainty, and reporting decisions.
- Convert lessons learned into assigned corrective actions with owners and due dates.
- Review incident-response metrics for bottlenecks without rewarding premature closure.
- Update the plan after material technology, provider, staffing, contract, and organizational changes.

Review Questions

1. Why is incident response both a technical capability and a governance capability for an MSP-supported contractor?

2. What is the practical difference between a security event and a cybersecurity incident?

3. Why should a SOC severity label not determine whether an event is contractually reportable?

4. What decision rights should be established before a serious incident occurs?

5. Why should incident plans be built around real systems and providers rather than abstract phases alone?

6. What makes alternate communications important during an identity or email incident?

7. Why should cyber-reporting clauses be mapped by contract before an incident?

8. How should customer and provider responsibilities be divided without transferring contractor accountability?

9. Why should monitoring coverage be reconciled with the asset and CUI-scope inventories?

10. How should user-reported suspicious activity enter the incident workflow?

11. What evidence should analysts correlate during initial triage?

12. How can severity classification help without replacing professional judgment?

13. Why must incident scope be revisited as new evidence appears?

14. How should an organization evaluate possible CUI or covered-defense-information impact?

15. What is the appropriate role of threat intelligence in an active investigation?

16. What factors should influence a containment decision?

17. Why is a password reset alone often insufficient for identity compromise?

18. What should happen before an endpoint is reimaged after a serious malware incident?

19. What additional paths should be examined during remote-access or network compromise?

20. Why does use of a cloud provider not remove the customer’s incident responsibilities?

21. What should be checked after a phishing or business-email-compromise event?

22. Why does ransomware place unusual pressure on evidence and recovery decisions?

23. Why do privileged-user incidents sometimes require restricted handling?

24. What does forensic readiness provide before an incident occurs?

25. What information should an evidence register preserve?

26. Under DFARS 252.204-7012, what categories of media and monitoring information are subject to the clause’s 90-day preservation requirement?

27. How should malicious software connected to a reported incident be handled under the applicable DFARS instructions?

28. Why should an incident timeline normalize time zones and source references?

29. Why should technical responders not make every external communication decision?

30. What does rapidly report mean under DFARS 252.204-7012?

31. Why should portal access and reporting prerequisites be tested before an incident?

32. How can subcontractor delays affect a prime contractor’s reporting timeline?

33. What should an organization expect after a cyber-incident report is submitted?

34. What distinguishes eradication from containment?

35. What security checks should occur before return to service?

36. How can backup restoration reintroduce an incident?

37. Why is enhanced monitoring appropriate after recovery?

38. What makes a lessons-learned process operationally useful?

39. Why can simplistic incident metrics create harmful incentives?

40. What changes should trigger review of the incident-response plan?

Answer Guidance

Questions 1 through 8 focus on governance, terminology, authority, planning, communications, contracts, and shared responsibility. Strong answers should emphasize that providers can perform important technical functions while the

contractor retains responsibility for understanding and satisfying the obligations that apply to its own contracts.

Questions 9 through 15 focus on detection, triage, severity, scope, information impact, and threat context. Strong answers should distinguish observed facts from assumptions and should explain why alert labels, threat intelligence, and early scope are inputs to judgment rather than final conclusions.

Questions 16 through 23 focus on containment patterns for identity, endpoint, network, cloud, email, ransomware, and privileged activity. Strong answers should balance interruption of harmful activity with evidence preservation, business continuity, and the need to eliminate persistent access.

Questions 24 through 33 focus on forensic readiness, evidence integrity, DFARS reporting, preservation, malware handling, timelines, communications, submission readiness, subcontractors, and government follow-up. Strong answers should use the exact clause and current reporting instructions when a contractual statement is required and should avoid generalizing one contract's obligations to every environment.

Questions 34 through 40 focus on eradication, recovery, backups, enhanced monitoring, lessons learned, metrics, and sustainment. Strong answers should show how an incident feeds back into configuration, vulnerability, identity, logging, training, contracts, and provider management rather than ending when systems return to service.

Key Terms

Cyber Incident: Under the applicable contractual or organizational definition, an event that requires cybersecurity incident handling and may trigger internal or external obligations. Always use the governing definition for a specific decision.

Discovery Time: The recorded point at which the organization discovered the cyber incident for purposes of the applicable reporting process; it should be preserved carefully when a reporting timeline depends on it.

Rapidly Report: In DFARS 252.204-7012, within 72 hours of discovery of any cyber incident when the clause applies.

Incident Commander: The person assigned authority to coordinate the incident response, decisions, priorities, and communication across participating teams.

Triage: The initial process of validating an event, collecting facts, estimating significance, and deciding escalation and next investigative actions.

Containment: Actions taken to limit ongoing damage or unauthorized activity while preserving needed evidence and supporting mission priorities.

Eradication: Removal of the cause, persistence, malicious components, compromised credentials, or exploited weaknesses that allowed the incident to continue.

Recovery: Controlled restoration and return to service with verification that systems are functional, protected, and appropriately monitored.

Forensic Readiness: Preparation of logging, tooling, retention, authority, skills, and evidence procedures so that useful investigation can begin quickly when an incident occurs.

Evidence Register: A controlled record that identifies incident artifacts, their source, collection details, storage location, custodian, and relevant integrity or access information.

Chain of Custody: A record of possession, transfer, handling, and control of evidence used when the investigative or legal context requires that level of traceability.

Indicator of Compromise (IOC): An observed artifact or pattern that may be associated with malicious activity and can support searching or detection; an IOC alone is not proof of attribution.

Out-of-Band Communication: A communication method independent of potentially compromised primary enterprise services.

Severity: An internal classification used to prioritize response based on impact, scope, urgency, criticality, and other organizational criteria.

Customer Responsibility Matrix: A documented allocation of customer and provider responsibilities that can include incident detection, escalation, containment, evidence, reporting support, and recovery.

Enhanced Monitoring: A temporary period of increased detection and review after containment or recovery to identify recurrence, persistence, or related activity.

Lessons Learned: A structured review that converts observations from incidents or exercises into owned improvements to technology, process, people, contracts, or documentation.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Use the current edition and applicable provisions for CMMC program requirements, assessment status, scope, external service providers, and affirmation.

R2. National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Incident Response requirements 3.6.1, 3.6.2, and 3.6.3 form the Level 2 baseline discussed in this chapter.

R3. National Institute of Standards and Technology. NIST SP 800-171A, June 2018, Assessing Security Requirements for Controlled Unclassified Information. Use the applicable assessment objectives and examine, interview, and test methods for the Revision 2 requirements referenced by the current CMMC Level 2 framework.

R4. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (current clause text). The clause defines rapidly report as within 72 hours of discovery of any cyber incident, addresses cyber-incident reporting, malicious-software submission, preservation and protection of affected-system images and relevant monitoring/packet-capture data for at least 90 days from report submission, and access to additional information or equipment for forensic analysis when requested by DoD.

R5. National Institute of Standards and Technology. NIST SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, April 2025. Revision 3 superseded SP 800-61 Revision 2 and integrates incident response across cybersecurity risk management.

R6. Department CMMC resources and announcements. On July 13, 2026, the Department announced immediate suspension of CMMC Phase II requirements while Phase I self-assessment requirements remain in place. Confirm current implementation status, reporting instructions, and acquisition guidance before relying on dates or procedures.

R7. The organization’s actual solicitations, contracts, task orders, subcontracts, reporting instructions, and provider agreements. These are necessary to determine which reporting clauses, timelines, flow-down duties, and communication requirements apply to a specific incident.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance for readiness and incident-response program design. It does not replace governing regulations, contractual clauses, current reporting instructions, legal advice, insurer requirements, law-enforcement guidance, or an authorized CMMC assessment determination.

Chapter Closing

Incident response is where the quality of the security program becomes visible under pressure. Logging and monitoring reveal what is happening. Configuration and vulnerability management reduce the weaknesses that can be exploited. Identity, access, network, endpoint, cloud, backup, and provider controls limit the damage. But when a serious event occurs, those capabilities must be coordinated through a response process that can make decisions, preserve evidence, meet obligations, and restore mission operations.

For an MSP, the central lesson is that shared technology does not eliminate customer accountability. The provider can detect, investigate, contain, preserve, and restore. The customer still needs to understand what happened in its environment, determine what information and contracts were affected, make required decisions, and retain evidence that the process worked. The responsibility model must allow both organizations to move quickly without confusing assistance with accountability.

A mature response program therefore does not measure success only by how fast an alert was closed. It asks whether the right event was recognized, whether the scope was correct, whether evidence survived, whether communications were controlled, whether contractual requirements were met, whether recovery was safe, and whether the weakness that enabled the incident was actually corrected. When those disciplines operate together, incident response becomes more than an emergency procedure. It becomes a continuing part of the organization’s cybersecurity and CMMC readiness.

CMMC for MSPs

From Readiness to Certification

Chapter 14

Evidence: Proving That the Controls Work

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Focus

How an MSP-supported organization turns routine security operations into credible, customer-specific evidence that demonstrates sustained implementation - not merely a collection of screenshots prepared for assessment week.

Chapter Contents

- Purpose, learning objectives, source context, and evidence operating principles
- 14.1–14.9 What makes evidence credible, current, attributable, and useful
- 14.10–14.16 Evidence architecture, repositories, retention, and shared responsibility
- 14.17–14.33 Control-family evidence patterns across MSP-supported environments
- 14.34–14.44 Tickets, screenshots, exports, interviews, demonstrations, refresh, and assessor requests
- 14.45–14.48 Harbor Point case studies and the continuous evidence operating model
- Evidence field guide, implementation checklist, workshops, review questions, key terms, and official references

Chapter Purpose

Chapter 9 organized the evidence package for assessment readiness. Chapter 14 goes deeper into a different question: what does the organization need to preserve during ordinary operations so that it can prove, later and under scrutiny, that a security requirement was actually implemented and sustained? That distinction matters because evidence assembled after the fact can look polished while still failing to show what happened during the period being evaluated.

For an MSP-supported organization, the evidence problem is distributed. Harbor Point Engineering may approve access, NorthStar may implement the configuration, Beacon Security Operations may monitor the event, a cloud provider may generate the audit record, and a business owner may accept an exception. The useful record is therefore rarely one screenshot. It is a connected set of authoritative artifacts that shows the requirement, the responsible parties, the affected population, the action taken, the time period, the result, and the way exceptions were handled.

This chapter treats evidence as an operational design problem. We will examine how tickets, logs, approvals, configuration exports, vulnerability records, incident cases, identity reports, training records, physical-access records, cloud telemetry, backup results, and provider reports can become dependable proof when they are created by controlled processes. We will also examine common weak patterns: undated screenshots, generic vendor attestations, exports without scope context, reports that cover only a sample while being described as the full population, and evidence that cannot be tied to the customer or time period.

The central principle is simple: evidence should be the natural exhaust of a functioning control. Assessment preparation may organize that evidence, but it should not manufacture the history that the operating process failed to create.

Learning Objectives

- Distinguish source evidence, presentation evidence, narrative explanation, and management attestation.
- Evaluate evidence for relevance, attribution, currency, completeness, authenticity, consistency, and retrievability.
- Connect assessment objectives to evidence sources before collecting artifacts.
- Design evidence repositories and indexes that preserve customer, system, time-period, custodian, and control context.
- Use tickets, logs, configuration records, approvals, and system-generated exports to demonstrate recurring control operation.

- Build customer-specific evidence from multi-tenant MSP, MSSP, RMM, PSA, SIEM, EDR, and cloud platforms without exposing other customers.
- Identify strong evidence patterns for access, authentication, audit, configuration, vulnerability, incident response, backups, media, physical security, maintenance, and training.
- Prepare interviews and technical demonstrations that confirm the same facts shown by documentary evidence.
- Resolve contradictory, missing, stale, or incomplete evidence without manufacturing retroactive proof.
- Operate a continuous evidence program that survives personnel changes, provider transitions, incidents, and assessment cycles.

Source Context and Applicability

The CMMC Level 2 framework discussed in this book is tied to the security requirements and assessment approach incorporated by the governing CMMC rule and applicable acquisition requirements. NIST SP 800-171 Revision 2 remains an important source for the 110-requirement baseline referenced in the current CMMC Level 2 framework, while the June 2018 SP 800-171A assessment procedures provide the Revision 2 assessment objectives and the examine, interview, and test methods used in that context. NIST has since published Revision 3 materials, including SP 800-171A Revision 3. Those newer publications are valuable for modern security and assessment practice, but readers must distinguish them from the specific source incorporated into an applicable CMMC assessment or contract.

Evidence practices must also reflect contract-specific obligations. DFARS 252.204-7012, when applicable, requires adequate security for covered contractor information systems and includes cyber-incident reporting, cloud, preservation, and forensic-access provisions. Those contractual duties can create evidence and retention needs that are separate from ordinary CMMC assessment preparation. Evidence retention should therefore be governed by the actual source that creates the obligation rather than by a universal period invented for convenience.

This chapter uses the fictional Harbor Point Engineering, NorthStar Managed Services, and Beacon Security Operations environment. The evidence structures, checklists, and workshop methods are practical operating models, not additional CMMC requirements. The organization should always confirm the current eCFR, acquisition clauses, solicitation, contract, and official CMMC guidance before relying on a regulatory interpretation.

Evidence quality	Operational question	Weak pattern
Relevance	Does the artifact address the exact requirement or assessment objective?	A policy is offered when the question is whether a setting is enabled.
Attribution	Can the record be tied to Harbor Point, its tenant, asset, user, or provider service?	Generic vendor material with no customer context.
Currency	Does it cover the time period being evaluated?	A current screenshot is used to prove a monthly process occurred all year.
Completeness	Does it represent the population or clearly describe the sample?	Five devices are shown without explaining that 380 are in scope.
Authenticity	Is the record traceable to an authoritative source?	Manually recreated spreadsheet with no source reference.
Consistency	Does it agree with other records and documented responsibilities?	Ticket says NorthStar owns the task; contract says customer owns it.
Retrievability	Can authorized personnel reproduce or obtain it reliably?	Only one engineer knows which query generated the report.

14.1 Evidence Is a Claim Supported by Observable Facts

Evidence is useful only when it supports a specific factual claim about implementation. A document can be authentic and still be irrelevant to the question being asked. A dashboard can be current and still fail to show whether the relevant population was covered. Harbor Point therefore writes the claim first, identifies the authoritative source that can support it, and only then decides which artifact should be retained or presented.

Operationally, the organization should define the evidence outcome before work begins. For evidence is a claim supported by observable facts, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

The strongest proof usually comes from corroboration. One artifact may show authorization, another may show technical implementation, and a third may show recurring monitoring or review. The evidence package should explain those

relationships directly rather than expecting an assessor or reviewer to infer them. When records disagree, the discrepancy is investigated as a potential control or scope issue instead of being hidden by selecting only the most favorable artifact.

A sustainable MSP model also considers personnel turnover and service transition. A backup engineer or successor provider should be able to locate the source, reproduce the report where permitted, understand the filters, and explain the customer-specific responsibility. If evidence depends on one technician remembering a special query or manually assembling a spreadsheet, the organization has identified an operational weakness even when the underlying technology is sound.

14.2 Start with the Assessment Objective, Not the Screenshot

Assessment objectives decompose broad requirements into facts that can be examined, discussed, or tested. NorthStar uses those facts to design its evidence outputs. This prevents the common mistake of collecting whatever is easy to export and hoping an assessor can infer the rest.

Operationally, the organization should define the evidence outcome before work begins. For start with the assessment objective, not the screenshot, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.3 Separate Source Evidence from Presentation Evidence

Source evidence is the authoritative record created by the system or process. Presentation evidence is a curated view used to explain that source. Both are useful, but they serve different purposes. A management dashboard can summarize patch health, while the deployment system, vulnerability platform, and exception records remain the underlying sources.

Operationally, the organization should define the evidence outcome before work begins. For separate source evidence from presentation evidence, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.4 Preserve Historical Evidence for Recurring Controls

Recurring controls must be demonstrated across time. If quarterly access reviews are required by the organization’s own process, a current membership list does not show that the earlier reviews occurred. Harbor Point preserves review dates, decisions, exceptions, and completion evidence so the history can be reconstructed without relying on memory.

Operationally, the organization should define the evidence outcome before work begins. For preserve historical evidence for recurring controls, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.5 Distinguish Population Evidence from Sample Evidence

Evidence should say whether it represents all in-scope items or a sample. A sample can support testing, but it must be selected from a known population. NorthStar therefore reconciles exported results to the asset, user, or system inventory before presenting coverage claims.

Operationally, the organization should define the evidence outcome before work begins. For distinguish population evidence from sample evidence, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.6 Establish Customer and System Attribution

Multi-tenant platforms make attribution especially important. An exported alert, device record, or administrator list should identify the customer tenant or other reliable scope marker. Provider-wide metrics may explain capability, but they do not prove the state of one customer environment.

Operationally, the organization should define the evidence outcome before work begins. For establish customer and system attribution, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence design element	Harbor Point operating rule
Claim to prove	Write the exact implementation fact before collecting artifacts.
Authoritative source	Identify the system or record that creates the fact during normal operations.
Population and period	State what assets/users/events and what dates the artifact covers.
Provider boundary	Identify which organization performs the action and which can produce the record.
Validation	Cross-check at least one independent record or safe test where appropriate.
Exception path	Show how deviations are approved, tracked, monitored, and closed.

14.7 Preserve Time Context and Synchronization

Evidence without time context is difficult to evaluate. Harbor Point records the generation date, the covered period, the timezone where relevant, and the source system. Synchronized system clocks also matter because incident, access, logging, and change evidence may need to be correlated across platforms.

Operationally, the organization should define the evidence outcome before work begins. For preserve time context and synchronization, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.8 Protect Evidence Integrity and Authenticity

The organization should preserve enough source context to show that an artifact is what it claims to be. This can include system-generated identifiers, export metadata, digital signatures, controlled repositories, hashes for selected high-value records, and role-based access to evidence stores. Not every screenshot requires forensic treatment, but critical evidence should not be casually editable without traceability.

Operationally, the organization should define the evidence outcome before work begins. For protect evidence integrity and authenticity, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected

population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.9 Use Chain of Custody When the Situation Requires It

Formal chain of custody is appropriate when evidence may support an investigation, legal matter, or contractual forensic request. Routine assessment screenshots generally do not need the same process. The key is to apply the stronger discipline when the nature of the record and the governing obligation require it.

Operationally, the organization should define the evidence outcome before work begins. For use chain of custody when the situation requires it, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.10 Build an Evidence Architecture Before the Assessment

Evidence readiness improves when sources are designed in advance. Harbor Point's evidence architecture maps each requirement or objective to systems, records, owners, custodians, retention, and retrieval paths. The architecture does not mean duplicating every record into one giant repository; it identifies where the authoritative source lives and how authorized people obtain it.

Operationally, the organization should define the evidence outcome before work begins. For build an evidence architecture before the assessment, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.11 Use a Controlled Naming and Indexing Model

A controlled index makes evidence discoverable. The index identifies requirement or objective, artifact description, tenant or system, period, source, custodian, sensitivity, retention rule, and storage location. File names help, but the index provides the relationships that a filename cannot carry reliably.

Operationally, the organization should define the evidence outcome before work begins. For use a controlled naming and indexing model, Harbor Point identifies the

responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.12 Protect the Evidence Repository as a Security Asset

Evidence can contain CUI, Security Protection Data, personal data, network diagrams, vulnerability details, and privileged-access information. The repository therefore deserves deliberate access control, logging, backup, and retention. An assessment folder should not become an uncontrolled shadow copy of the environment.

Operationally, the organization should define the evidence outcome before work begins. For protect the evidence repository as a security asset, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.13 Define Retention and Disposition by Record Type

Different records have different governing sources. Harbor Point uses a retention matrix instead of one universal number. Contractual incident evidence, HR records, audit logs, access approvals, and assessment working files may each have different obligations or business needs.

Operationally, the organization should define the evidence outcome before work begins. For define retention and disposition by record type, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.14 Produce Customer-Specific Evidence from Multi-Tenant Platforms

An MSP must be able to prove one customer’s state without exposing another customer. NorthStar designs tenant filters, customer-specific exports, scoped dashboards, and redaction procedures into normal service delivery. Last-minute manual filtering is error-prone and can itself create a confidentiality incident.

Operationally, the organization should define the evidence outcome before work begins. For produce customer-specific evidence from multi-tenant platforms, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence design element	Harbor Point operating rule
Claim to prove	Write the exact implementation fact before collecting artifacts.
Authoritative source	Identify the system or record that creates the fact during normal operations.
Population and period	State what assets/users/events and what dates the artifact covers.
Provider boundary	Identify which organization performs the action and which can produce the record.
Validation	Cross-check at least one independent record or safe test where appropriate.
Exception path	Show how deviations are approved, tracked, monitored, and closed.

14.15 Map Evidence Ownership in the Customer Responsibility Matrix

The Customer Responsibility Matrix should identify who performs the control and who can produce the evidence. Those roles may be different. Beacon may monitor alerts while NorthStar retains the case platform, and Harbor Point may retain final incident authority. Evidence ownership therefore belongs in the same shared-responsibility discussion as technical implementation.

Operationally, the organization should define the evidence outcome before work begins. For map evidence ownership in the customer responsibility matrix, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.16 Require Provider Evidence Service Levels

Evidence delivery is a service requirement. Contracts and operating procedures should identify what reports, logs, tickets, configuration records, and historical data the provider can produce, the retention available, expected response times, and any platform limitations. Without those terms, an otherwise capable provider may become an assessment bottleneck.

Operationally, the organization should define the evidence outcome before work begins. For require provider evidence service levels, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.17 Prove Access Control Through Requests, Decisions, and Effective State

Strong access-control evidence connects business authorization to technical state. Harbor Point preserves the request, approver, role, provisioning record, effective group membership, periodic review, and removal record. A current group screenshot proves only the current state; it does not prove why access was granted or whether it was reviewed.

Operationally, the organization should define the evidence outcome before work begins. For prove access control through requests, decisions, and effective state, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

Access request; approval; role mapping; effective membership; quarterly review; removal record

14.18 Prove Identification and Authentication Through Enrollment and Enforcement

Authentication evidence should show enrollment, enforcement, privileged treatment, exceptions, and lifecycle changes. NorthStar may provide tenant configuration exports and MFA registration data while Harbor Point provides user approval and exception decisions. Together they show both policy and operation.

Operationally, the organization should define the evidence outcome before work begins. For prove identification and authentication through enrollment and enforcement, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

MFA policy; enrollment report; privileged-account list; authentication policy; exception record

14.19 Prove Audit and Accountability Through the Full Logging Pipeline

Audit evidence should demonstrate more than the existence of a SIEM. Harbor Point traces selected events from source generation through collection, parsing, correlation, alert creation, analyst handling, retention, and review. This end-to-end pattern shows whether monitoring actually works.

Operationally, the organization should define the evidence outcome before work begins. For prove audit and accountability through the full logging pipeline, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

Log-source inventory; SIEM ingestion status; test event; alert case; retention configuration; review record

14.20 Prove Configuration Management Through Baselines and Drift Records

Configuration evidence begins with an approved baseline and continues with enforcement, drift detection, approved deviations, change records, and verification. NorthStar preserves configuration profiles and compliance reports, but those artifacts are tied back to the in-scope population and the approved baseline version.

Operationally, the organization should define the evidence outcome before work begins. For prove configuration management through baselines and drift records, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

Approved baseline; configuration profile; compliance report; drift alert; approved deviation; verification

14.21 Prove Vulnerability and Patch Management Through Population Reconciliation

A scanner report alone does not prove vulnerability management. Harbor Point preserves inventory reconciliation, scan coverage, findings, prioritization, remediation tickets, exceptions, deployment results, rescans, and closure. The evidence chain demonstrates that identified flaws enter a controlled process and are verified after correction.

Operationally, the organization should define the evidence outcome before work begins. For prove vulnerability and patch management through population reconciliation, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

Inventory reconciliation; scan coverage; finding; remediation ticket; deployment result; rescan; exception

Evidence design element	Harbor Point operating rule
Claim to prove	Write the exact implementation fact before collecting artifacts.
Authoritative source	Identify the system or record that creates the fact during normal operations.
Population and period	State what assets/users/events and what dates the artifact covers.
Provider boundary	Identify which organization performs the action and which can produce the record.
Validation	Cross-check at least one independent record or safe test where appropriate.
Exception path	Show how deviations are approved, tracked, monitored, and closed.

14.22 Prove Endpoint and Malicious-Code Protection Through Coverage and Response

Endpoint protection evidence should answer coverage and response questions. Which systems should have protection? Which are reporting? Are signatures or engines current? What happens when protection is disabled or malware is detected? NorthStar reconciles its security console to the customer inventory so missing agents are visible rather than silently excluded.

Operationally, the organization should define the evidence outcome before work begins. For prove endpoint and malicious-code protection through coverage and response, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.23 Prove Network Protection Through Rules, Paths, and Validation

Network evidence should connect architecture to effective rules and test results. A diagram describes intended paths; firewall and network-device records show configured enforcement; change tickets explain why rules changed; validation demonstrates that prohibited paths are actually blocked.

Operationally, the organization should define the evidence outcome before work begins. For prove network protection through rules, paths, and validation, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.24 Prove Encryption and Key Management Without Exposing Secrets

Cryptographic evidence must prove use without exposing keys or secrets unnecessarily. Configuration records, policy settings, certificate metadata, approved cryptographic modules, and controlled test results can show the relevant protection. Secret material should remain protected and should not be copied into an evidence package merely for completeness.

Operationally, the organization should define the evidence outcome before work begins. For prove encryption and key management without exposing secrets, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.25 Prove Email and Collaboration Controls Through Tenant Configuration

Email and collaboration platforms often hold both CUI-related workflows and security administration functions. Evidence should identify the tenant, relevant security settings, sharing rules, external collaboration controls, audit capability, retention, and administrative roles rather than relying on generic product certifications.

Operationally, the organization should define the evidence outcome before work begins. For prove email and collaboration controls through tenant configuration,

Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.26 Prove Cloud Controls Through Shared-Responsibility Evidence

Cloud evidence is inherently shared. Provider assurance may support inherited responsibilities, while Harbor Point still needs evidence of tenant configuration, identity, network, logging, data handling, and customer-managed settings. The evidence package should make that boundary explicit.

Operationally, the organization should define the evidence outcome before work begins. For prove cloud controls through shared-responsibility evidence, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

Provider assurance; tenant configuration; responsibility matrix; identity settings; logging; network rules; evidence export

14.27 Prove Backup and Recovery Through Restore Evidence

Backup evidence must include successful protection of the expected population and a demonstrated ability to restore. NorthStar therefore preserves job coverage, failure handling, restore tests, authorization, destination controls, and post-restore cleanup. A green backup dashboard without restore evidence shows only part of the control.

Operationally, the organization should define the evidence outcome before work begins. For prove backup and recovery through restore evidence, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

Protected population; job history; failure tickets; restore authorization; restore test;

validation; cleanup record

14.28 Prove Incident Response Through Cases, Timelines, and Exercises

Incident-response evidence should preserve the case record, timeline, affected systems and accounts, containment actions, decision authority, communications, required reporting, forensic preservation, recovery validation, and lessons learned. Exercises should also produce records that show the capability was tested before a real crisis.

Operationally, the organization should define the evidence outcome before work begins. For prove incident response through cases, timelines, and exercises, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence to Preserve

Incident case; timeline; containment evidence; preserved data; reporting decision; recovery validation; lessons learned

Evidence design element	Harbor Point operating rule
Claim to prove	Write the exact implementation fact before collecting artifacts.
Authoritative source	Identify the system or record that creates the fact during normal operations.
Population and period	State what assets/users/events and what dates the artifact covers.
Provider boundary	Identify which organization performs the action and which can produce the record.
Validation	Cross-check at least one independent record or safe test where appropriate.
Exception path	Show how deviations are approved, tracked, monitored, and closed.

14.29 Prove Training and Personnel Security Through Lifecycle Records

Training and personnel-security evidence should follow the user lifecycle. Harbor Point preserves assignment, completion, role-specific training, acknowledgement, screening or onboarding records where applicable, and termination/offboarding actions. The evidence should distinguish policy existence from actual completion by the relevant people.

Operationally, the organization should define the evidence outcome before work begins. For prove training and personnel security through lifecycle records, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.30 Prove Physical Protection Through Access and Visitor Records

Physical-security evidence should show controlled access, visitor handling, access-device issuance, reviews, and response to lost or revoked credentials. A visitor log becomes stronger when the organization can explain escort rules, access boundaries, and badge recovery.

Operationally, the organization should define the evidence outcome before work begins. For prove physical protection through access and visitor records, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.31 Prove Media Protection Through Handling and Sanitization Records

Media evidence follows information through receipt, use, transport, storage, reuse, sanitization, and disposal. Harbor Point records approvals and sanitization or destruction results so the organization can demonstrate what happened to the specific media, not merely cite a procedure.

Operationally, the organization should define the evidence outcome before work begins. For prove media protection through handling and sanitization records, Harbor Point identifies the responsible process owner, the authoritative system of record, the

expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.32 Prove Maintenance and Remote Support Through Controlled Sessions

Maintenance and remote support create short-lived privileged pathways. Evidence should identify who was authorized, what system was accessed, the approved method, session timing, actions performed, monitoring, and closure. Provider remote-management tools should produce customer-specific records that can be reconciled to tickets and privileged accounts.

Operationally, the organization should define the evidence outcome before work begins. For prove maintenance and remote support through controlled sessions, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.33 Prove Change Management Through Approval, Implementation, and Verification

Change evidence connects request, risk, approval, implementation, testing, rollback, and final verification. Emergency changes need the same factual history even when approval timing differs. Harbor Point uses change records to explain why the environment differs from an earlier baseline and to show that security impact was considered.

Operationally, the organization should define the evidence outcome before work begins. For prove change management through approval, implementation, and verification, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.34 Use Tickets as Evidence Without Treating the Ticket as the Control

Tickets are valuable because they connect people, systems, time, approvals, and actions. But a ticket stating “MFA enabled” does not prove the setting. NorthStar treats tickets as workflow evidence and links them to configuration or system-generated results that prove the technical outcome.

Operationally, the organization should define the evidence outcome before work begins. For use tickets as evidence without treating the ticket as the control, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.35 Use Screenshots Carefully and Preserve Their Context

Screenshots are easy to create and easy to misunderstand. A useful screenshot includes enough interface context to identify the system, tenant, relevant setting, and date when possible. Cropping should not remove attribution, and screenshots should not replace authoritative exports or historical records when those are available.

Operationally, the organization should define the evidence outcome before work begins. For use screenshots carefully and preserve their context, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence design element	Harbor Point operating rule
Claim to prove	Write the exact implementation fact before collecting artifacts.
Authoritative source	Identify the system or record that creates the fact during normal operations.
Population and period	State what assets/users/events and what dates the artifact covers.
Provider boundary	Identify which organization performs the action and which can produce the record.
Validation	Cross-check at least one independent record or safe test where appropriate.

Evidence design element	Harbor Point operating rule
Exception path	Show how deviations are approved, tracked, monitored, and closed.

14.36 Use Exports, APIs, and Reports Reproducibly

Exports and APIs can produce stronger evidence when they are reproducible. Harbor Point records the query, filters, tenant, population, period, timezone, and generation method. This allows another authorized person to reproduce the result and reduces dependence on one analyst’s undocumented knowledge.

Operationally, the organization should define the evidence outcome before work begins. For use exports, apis, and reports reproducibly, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.37 Prepare Interviews to Explain Real Workflows

Interviews confirm how people understand and perform the process. Preparation should focus on real workflows, responsibilities, exceptions, and evidence sources. Scripted answers can hide uncertainty and break down when follow-up questions move beyond memorized language.

Operationally, the organization should define the evidence outcome before work begins. For prepare interviews to explain real workflows, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.38 Design Technical Demonstrations That Answer a Defined Question

A technical demonstration should answer a defined question safely. Harbor Point uses test accounts, benign events, designated data, and customer-scoped views where appropriate. The demonstration should show the control operating without creating unnecessary production risk or cross-customer exposure.

Operationally, the organization should define the evidence outcome before work begins. For design technical demonstrations that answer a defined question, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.39 Refresh Evidence on a Risk-Based Cadence

Evidence has a useful life. High-change controls such as privileged access, vulnerability status, endpoints, and cloud configuration may need more frequent refresh than stable governance documents. Harbor Point ties refresh to both cadence and change triggers so major events do not wait for the next scheduled review.

Operationally, the organization should define the evidence outcome before work begins. For refresh evidence on a risk-based cadence, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.40 Reconcile Contradictory Evidence Before Assessment

Contradictory evidence is a signal to investigate, not an inconvenience to hide. If the asset inventory lists a server that the EDR console does not show, or a contract assigns a task differently from the responsibility matrix, the team resolves the underlying condition and records the outcome before assessment.

Operationally, the organization should define the evidence outcome before work begins. For reconcile contradictory evidence before assessment, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.41 Handle Missing Evidence Without Manufacturing History

When historical evidence is missing, the organization should state the limitation accurately, correct the process, and begin generating reliable records going forward. Recreating old approvals or backdating records undermines credibility and can create legal or ethical problems. The goal is to improve the control and the evidence process, not to manufacture a cleaner past.

Operationally, the organization should define the evidence outcome before work begins. For handle missing evidence without manufacturing history, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.42 Build Evidence Requirements into MSP Service Delivery

Evidence should be part of the service catalog. NorthStar defines which customer-specific reports are produced automatically, which require a request, which are retained by the provider, and which the customer must archive. Service design also identifies dependencies such as licensing tiers and historical-retention limits.

Operationally, the organization should define the evidence outcome before work begins. For build evidence requirements into msp service delivery, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence design element	Harbor Point operating rule
Claim to prove	Write the exact implementation fact before collecting artifacts.
Authoritative source	Identify the system or record that creates the fact during normal operations.
Population and period	State what assets/users/events and what dates the artifact covers.
Provider boundary	Identify which organization performs the action and which can produce the record.
Validation	Cross-check at least one independent record or safe test where appropriate.
Exception path	Show how deviations are approved, tracked, monitored, and closed.

14.43 Control the Assessor Evidence-Request Workflow

Assessment evidence requests should flow through a controlled tracker so the organization knows what was requested, who owns the response, which artifact was

released, what version was provided, and whether sensitive information was minimized. One controlled release process reduces duplication and conflicting submissions.

Operationally, the organization should define the evidence outcome before work begins. For control the assessor evidence-request workflow, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.44 Give Executives Evidence They Can Govern

Executives need evidence that supports decisions rather than raw technical volume. Harbor Point's governance package highlights material exceptions, overdue reviews, unresolved provider limitations, recurring control failures, evidence aging, and major changes. The underlying records remain available for technical review.

Operationally, the organization should define the evidence outcome before work begins. For give executives evidence they can govern, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.45 Harbor Point Case Study: Proving Privileged Access Review

Harbor Point discovers that the quarterly privileged-access review packet contains an exported group list but no record of reviewer decisions. The group state is technically correct, yet the evidence does not prove the review process occurred as designed. The team redesigns the review so each decision, exception, and removal is captured in the access-governance workflow.

Operationally, the organization should define the evidence outcome before work begins. For harbor point case study: proving privileged access review, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.46 Harbor Point Case Study: Multi-Tenant SOC Evidence Without Cross-Customer Exposure

Beacon can display Harbor Point alerts in its analyst console, but the standard PDF report contains metrics aggregated across several customers. That report proves Beacon operates a SOC; it does not prove Harbor Point's alert handling. Beacon and NorthStar implement tenant-scoped exports with case identifiers, severity, timestamps, disposition, escalation, and service-level results.

Operationally, the organization should define the evidence outcome before work begins. For harbor point case study: multi-tenant soc evidence without cross-customer exposure, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.47 Harbor Point Case Study: Patching, Incident Response, and a Contradictory Timeline

A critical vulnerability appears closed in the patch platform, but incident telemetry shows exploitation attempts against one system after the recorded deployment time. The team discovers that the deployment job succeeded but the host reboot did not occur, leaving the vulnerable component active. Reconciling patch, vulnerability, endpoint, incident, and change evidence reveals the true timeline.

Operationally, the organization should define the evidence outcome before work begins. For harbor point case study: patching, incident response, and a contradictory timeline, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

14.48 Operate Evidence Readiness as a Continuous Service

Continuous evidence readiness is a service, not a folder. Harbor Point, NorthStar, and Beacon assign owners, define authoritative sources, automate repeatable exports, test retrieval, monitor evidence health, and review provider limitations. Assessment preparation then becomes a controlled selection and explanation process rather than a reconstruction project.

Operationally, the organization should define the evidence outcome before work begins. For operate evidence readiness as a continuous service, Harbor Point identifies the responsible process owner, the authoritative system of record, the expected population, and the event or cadence that should create a record. NorthStar and Beacon then align their runbooks so provider-generated records carry enough customer and time context to be useful without exposing unrelated tenants or secrets.

Evidence Field Guide for MSP-Supported Organizations

Area	Strong evidence pattern	Common weak pattern
Identity and access	Requests, approvals, effective membership, MFA, privileged roles, reviews, revocations	Current group screenshot with no authorization history
Logging/SOC	Source inventory, ingestion status, alert cases, analyst decisions, retention, test events	SIEM license or dashboard home page
Configuration	Approved baseline, enforced profile, drift, deviations, verification	Policy document without effective settings
Vulnerability/Patching	Coverage, findings, priority, remediation, deployment, rescan, exception	Scanner report with no closure trail
Incident response	Case, timeline, evidence preservation, decisions, reports, recovery, lessons	Tabletop slide deck with no action tracking
Cloud	Provider assurance plus tenant-specific configuration and logs	Vendor compliance brochure
Backups	Expected population, job health, failure handling, restore test	Green status screen with no restore proof
Training	Assignment, completion, role-specific content, overdue handling	Training policy only
Physical	Authorized list, visitor records, badge lifecycle, reviews	Uncontrolled sign-in sheet
Provider services	CRM, service description, tenant evidence, SLA, limitations	Generic MSP attestation

Chapter 14 Implementation Checklist

- Create an evidence-source map tied to the applicable requirements and assessment objectives.
- Identify authoritative sources rather than relying on assessment copies as the system of record.
- Assign primary and backup evidence custodians for critical sources.
- Record customer/tenant, system, population, time period, source, and custodian in the evidence index.
- Distinguish population evidence from samples and document the sampling basis.
- Preserve recurring-control history according to approved retention rules.
- Protect evidence repositories according to the sensitivity of the information they contain.
- Build customer-specific exports for multi-tenant MSP and MSSP platforms.
- Add evidence ownership and delivery expectations to the Customer Responsibility Matrix.
- Define provider evidence SLAs, retention, licensing dependencies, and offboarding portability.
- Reconcile access evidence from request through provisioning, review, and removal.
- Reconcile security-console coverage to the authoritative asset population.
- Test logging pipelines end to end and preserve the test result.
- Link configuration baselines to drift, approved deviations, and verification.
- Link vulnerability findings to remediation, rescan, and exception records.
- Preserve incident timelines and contractual reporting decisions with source evidence.
- Record backup restore tests, not only successful backup jobs.
- Use screenshots only when they preserve enough context to identify the relevant fact.
- Document queries and filters for exported or API-generated evidence so results are reproducible.
- Prepare interviewees around actual workflows rather than memorized compliance language.
- Use safe technical demonstrations to confirm documentary evidence.
- Investigate contradictory evidence and correct the underlying condition.
- Do not backdate, recreate, or manufacture historical records to fill gaps.
- Establish risk-based evidence refresh cadences and material-change triggers.

- Use one controlled evidence-request tracker during assessment activity.
- Conduct an evidence-health review as part of recurring CMMC governance.

Operational Workshops

Workshop 1 - Access Evidence Trace

Select one privileged account and trace the business request, approval, provisioning, effective membership, authentication protection, quarterly review, and current state. Record any break in the evidence chain.

Workshop 2 - Endpoint Coverage Reconciliation

Compare the current in-scope asset inventory to EDR, vulnerability, patch, encryption, and logging consoles. Explain every missing or duplicate record.

Workshop 3 - SIEM Test Event

Generate a benign event and follow it from the source system through collection, parsing, correlation, alerting, case creation, analyst action, and retention.

Workshop 4 - Multi-Tenant Export

Produce a Harbor Point report from a shared provider platform and verify that it contains sufficient customer context while exposing no other tenant data.

Workshop 5 - Historical Control Proof

Choose a recurring process such as quarterly access review or monthly vulnerability review and retrieve evidence from multiple prior cycles.

Workshop 6 - Backup Restore Evidence

Perform or review a controlled restore and preserve authorization, source, destination, result, integrity validation, and cleanup evidence.

Workshop 7 - Contradiction Drill

Intentionally compare inventory, endpoint, vulnerability, patch, and SIEM sources and resolve one inconsistency using documented ownership and source-of-truth rules.

Workshop 8 - Provider Evidence SLA Test

Request a customer-specific artifact from each critical provider and measure whether it arrives within the agreed time, scope, and format.

Workshop 9 - Evidence Request Simulation

Run a mock assessor request through intake, assignment, collection, review, minimization, approval, release, and tracker closure.

Workshop 10 - Missing Evidence Decision

Select a control with incomplete history. Document what can be proven, what cannot, what corrective action begins now, and how future evidence will be generated without creating retroactive records.

Review Questions

30. What is the difference between a control claim and the artifact used to support it?
31. Why should evidence collection begin with the assessment objective?
32. What is source evidence, and how does it differ from presentation evidence?
33. Why is a current screenshot weak evidence for a recurring control?
34. How should population evidence and sample evidence be distinguished?
35. What information establishes customer or tenant attribution?
36. Why do timestamps and time synchronization matter?
37. When is chain of custody appropriate?
38. What should an evidence architecture contain?
39. Why should the evidence repository be treated as a security asset?
40. Why should retention be determined by record type and governing source?
41. How can an MSP produce evidence from a multi-tenant platform safely?
42. Why should the Customer Responsibility Matrix include evidence ownership?
43. What belongs in an evidence service-level agreement?
44. What combination of records best proves access control?
45. What should authentication evidence show beyond a policy statement?
46. How can an organization prove that the logging pipeline works end to end?
47. What evidence demonstrates configuration drift management?
48. Why is a vulnerability scanner report insufficient by itself?
49. How should endpoint-protection coverage be reconciled?
50. What combination of records demonstrates network protection?
51. How can encryption be demonstrated without exposing secrets?
52. Why is provider assurance insufficient for cloud controls by itself?
53. What distinguishes backup evidence from recovery evidence?
54. What records make an incident-response case useful as evidence?
55. How should training evidence follow the user lifecycle?

56. What records support physical-security implementation?
57. What does strong media-sanitization evidence contain?
58. What should remote-maintenance evidence identify?
59. How does change-management evidence explain deviations from baselines?
60. Why should a ticket not be treated as the technical control itself?
61. What context should be preserved with a screenshot?
62. What makes an exported report reproducible?
63. How should personnel prepare for assessment interviews?
64. What makes a technical demonstration safe and useful?
65. How should evidence refresh frequency be determined?
66. What should the team do when two authoritative sources conflict?
67. How should missing historical evidence be handled?
68. Why should evidence requirements be designed into MSP services?
69. What does continuous evidence readiness look like after the assessment ends?

Answer Guidance

Questions 1 through 10 focus on evidence fundamentals. Strong evidence begins with a precise claim or assessment objective, uses authoritative sources, identifies population and time period, preserves attribution, and is stored in a controlled and retrievable manner. Presentation artifacts may improve explanation but should not obscure the source record.

Questions 11 through 20 focus on MSP delivery and technical controls. Retention must come from the governing source, provider evidence must be customer-specific, shared responsibilities must be explicit, and technical claims should be corroborated across authorization, effective state, coverage, monitoring, remediation, and verification records.

Questions 21 through 30 focus on domain-specific evidence. Network, encryption, cloud, recovery, incident response, personnel, physical security, media, maintenance, and change management each produce different records. The evidence pattern should follow the real workflow rather than forcing every control into the same screenshot-based template.

Questions 31 through 40 focus on evidence operations and sustainment. Tickets and screenshots are supporting artifacts, exports should be reproducible, interviews and demonstrations should confirm real processes, contradictions should trigger investigation, missing history should not be manufactured, and evidence generation should be designed into normal MSP service delivery.

Key Terms

Term	Working meaning
Assessment Objective	A specific fact or condition used to evaluate whether a security requirement is satisfied.
Authoritative Source	The system, record, or approved repository considered the primary source for a fact.
Corroborating Evidence	Independent evidence that supports or validates a claim shown by another source.
Evidence Architecture	The designed relationship among requirements, sources, owners, custodians, retention, repositories, and retrieval paths.
Evidence Custodian	The person or role responsible for preserving and retrieving designated evidence without necessarily owning the underlying control.
Evidence Index	A structured catalog that connects artifacts to objectives, scope, time period, source, custodian, sensitivity, and location.
Population Evidence	Evidence describing the complete set of relevant assets, users, events, or records for a defined period.
Presentation Evidence	A curated report, screenshot, summary, or view used to explain authoritative source evidence.
Source Evidence	The original or authoritative record generated by the system or process being evaluated.
Traceability	The ability to connect an artifact to its source, context, responsible party, and relevant time period.
Tenant Attribution	Reliable context showing that provider-generated evidence applies to the specific customer environment.
Evidence Health	The degree to which expected evidence remains current, complete, retrievable, attributable, and consistent over time.

Official References

- R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. Use the current edition for applicable

CMMC program requirements, scoping, assessment, external service provider, affirmation, and POA&M provisions.

- R2. National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, including applicable updates. This remains an important source for the 110-requirement baseline referenced by the current CMMC Level 2 framework discussed in this book.
- R3. National Institute of Standards and Technology. NIST SP 800-171A, June 2018, Assessing Security Requirements for Controlled Unclassified Information. The Revision 2 assessment procedures define assessment objectives and examine, interview, and test methods used in the CMMC Level 2 context discussed here. NIST has withdrawn this publication in favor of Revision 3 for general NIST use; readers must distinguish the current NIST publication from the assessment source incorporated by their governing CMMC process.
- R4. National Institute of Standards and Technology. NIST SP 800-171A Revision 3, May 2024. Use as a current NIST reference for modern assessment practice where appropriate, while verifying whether it is the governing assessment source for the specific CMMC or contract context.
- R5. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Review the current clause and the organization’s actual contract for safeguarding, cloud, reporting, preservation, and forensic-access obligations.
- R6. DFARS 252.204-7019 and 252.204-7020, as applicable, for NIST SP 800-171 DoD assessment requirements and related records.
- R7. Current Department of Defense CMMC resources, FAQs, implementation announcements, and applicable Cyber AB assessment-process materials. Confirm current program status and procedural requirements before assessment activity.
- R8. Applicable provider contracts, security service descriptions, Customer Responsibility Matrix, System Security Plan, internal policies, and evidence-retention schedules. These organizational records define how responsibilities and evidence are implemented in the actual environment.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance. It does not replace governing regulations, the organization’s actual solicitation or contract, legal advice, or an authorized CMMC assessment determination.

Chapter Closing

Evidence is not the control, but it is the organization's ability to demonstrate what the control actually did. A mature program does not begin evidence collection when the assessor schedules interviews. It designs workflows so approvals, technical state, monitoring, exceptions, changes, tests, and corrections naturally create reliable records throughout the year.

For an MSP, the challenge is to make that evidence both scalable and customer-specific. Shared platforms can automate security for hundreds of customers, but assessment accountability still requires Harbor Point to explain its own environment and NorthStar or Beacon to produce records that apply specifically to Harbor Point. Generic capability claims are helpful context; they are not a substitute for tenant-level proof.

The practical test is whether another authorized person can reconstruct the security story from authoritative records without relying on memory or manufacturing history. When that is possible, evidence readiness becomes an indicator of operational maturity. When it is not, the evidence gap often reveals a deeper process, responsibility, or control weakness that deserves correction.

Applied Evidence Playbooks and Templates

The following playbooks translate the chapter principles into repeatable operating patterns. Each playbook begins with a claim that an MSP-supported organization may need to demonstrate, identifies strong source records, highlights corroborating evidence, and describes validation steps. These are practical working models rather than additional CMMC requirements. The exact evidence should be selected according to the applicable requirement, assessment objective, contract, technology, and environment.

Playbook A - Privileged Access

Claim: only authorized personnel receive privileged access, the access is appropriately protected, reviewed, and removed when no longer required.

Primary evidence pattern:

- Approved access request and business justification
- Role or group mapping showing intended privilege
- System-generated effective membership or role assignment
- MFA or strong-authentication enforcement evidence
- Quarterly or event-driven review decisions

- Termination, transfer, or revocation record

Validation: select at least one current administrator, one recently removed administrator, and one service or emergency account. Trace each record from authorization through effective state and, where relevant, removal. Reconcile privileged groups to the identity inventory rather than relying on a manually maintained list.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook B - Account Lifecycle

Claim: accounts are created, changed, disabled, and removed through an authorized lifecycle.

Primary evidence pattern:

- Onboarding or change request
- Manager or data-owner approval
- Provisioning record
- Effective group/role membership
- Periodic review
- HR or contract end-date trigger
- Disablement/removal record

Validation: compare HR or authoritative personnel events to identity-platform actions. Look for orphaned accounts, delayed disablement, copied permissions,

dormant accounts, and exceptions. Preserve the evidence needed to explain both the expected process and any deviations.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook C - Logging and SOC Monitoring

Claim: required events are generated, centrally collected, retained, reviewed, correlated, and acted upon.

Primary evidence pattern:

- Log-source inventory
- Collector/agent health
- Ingestion or parsing status
- Benign test event
- Alert/correlation rule
- SOC case
- Analyst disposition
- Retention configuration

Validation: generate a controlled event and follow its identifiers across the entire pipeline. Confirm timestamps, tenant attribution, case creation, escalation, and closure. A SIEM dashboard that shows data volume should not be mistaken for proof that critical sources are complete or alerts are handled.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system,

	user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook D - Secure Configuration and Drift

Claim: systems are configured to an approved secure baseline and deviations are detected and governed.

Primary evidence pattern:

- Approved baseline version
- Configuration policy/profile
- Target population
- Compliance or drift report
- Change ticket
- Exception or deviation approval
- Post-change verification

Validation: choose several baseline settings and verify both intended configuration and effective state. Investigate devices that are excluded, stale, unenrolled, or reporting unknown status. Tie temporary deviations to owner, reason, expiration, and monitoring.

Evidence question	**Practical check**
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?

Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook E - Vulnerability and Patch Management

Claim: the organization discovers relevant flaws, prioritizes them, corrects them in a controlled manner, and verifies closure.

Primary evidence pattern:

- Asset inventory
- Scan coverage
- Finding record
- Risk/prioritization decision
- Remediation ticket
- Patch deployment result
- Reboot/restart evidence where relevant
- Rescan or verification
- Exception record

Validation: follow one critical and one moderate finding from discovery through closure. Confirm the affected asset remained in scope, the correction actually changed the vulnerable condition, and any exception was approved and monitored. Separate job success from security outcome.

Evidence question	**Practical check**
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-

	bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook F - Endpoint Security Coverage

Claim: endpoint protection is deployed to the expected population, remains current, and produces response actions when needed.

Primary evidence pattern:

- In-scope device inventory
- EDR/AV enrollment list
- Policy assignment
- Health/update status
- Tamper-protection setting
- Detection case
- Isolation or response action
- Coverage reconciliation

Validation: reconcile inventory to the endpoint platform and explain every exception. Test a benign detection or policy event where appropriate. The strongest evidence demonstrates both coverage and the operating response when an agent is missing or unhealthy.

Evidence question	**Practical check**
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook G - Cloud and SaaS Controls

Claim: the specific cloud service and customer tenant are configured and monitored in accordance with the organization's responsibility model.

Primary evidence pattern:

- Exact service/offering identification
- Provider assurance relevant to that offering
- Tenant configuration exports
- Admin-role list
- Identity and conditional-access settings
- Logging/audit configuration
- Data-sharing controls
- Customer/provider responsibility record

Validation: separate inherited provider capabilities from customer-configured controls. Confirm that the assurance material applies to the exact service in use and that tenant-specific evidence demonstrates the customer side of shared responsibility.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook H - Backup and Recovery

Claim: required systems and information are protected by backup and can be restored through a controlled process.

Primary evidence pattern:

- Expected protected population
- Backup job configuration
- Job history and failures
- Failure-remediation tickets
- Restore request/authorization
- Restore test result
- Integrity/application validation
- Cleanup record

Validation: choose a representative restore and confirm the destination is authorized, restored data is protected, validation occurred, and test copies were handled appropriately. Do not infer recoverability merely from successful backup jobs.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook I - Incident Response

Claim: the organization can detect, investigate, contain, report, recover from, and learn from security incidents.

Primary evidence pattern:

- Incident plan and contact roster
- SOC or user detection
- Case/timeline
- Affected-system/account analysis
- Containment evidence

- Preserved forensic data
- Contractual reporting decision
- Recovery validation
- Lessons learned and actions

Validation: compare the written plan to a real incident or exercise. Verify that authority, provider roles, evidence preservation, communications, and reporting decisions occurred as designed. Capture gaps as corrective actions rather than rewriting the history after the exercise.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook J - Security Training and Role Readiness

Claim: personnel receive required security awareness and role-specific preparation and overdue or missed training is managed.

Primary evidence pattern:

- Training assignment
- Course/content identifier
- Completion record
- Role-specific assignment
- Acknowledgment
- Overdue report
- Escalation or exception
- New-hire and termination lifecycle records

Validation: select current employees, recent hires, administrators, and one separated user. Confirm the training system and personnel records tell a consistent lifecycle story.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook K - Provider Evidence and Shared Responsibility

Claim: outsourced functions remain governed, customer-specific, and demonstrable.

Primary evidence pattern:

- Service description
- Customer Responsibility Matrix
- Contract/SLA
- Provider control evidence
- Customer-specific report
- Escalation/runbook
- Retention/export capability
- Provider-change notification

Validation: ask the provider to produce a historically relevant artifact within the agreed response time. Confirm that the evidence applies to the customer, protects other tenants, and can be tied to the provider responsibility described in the CRM.

Evidence question	Practical check
Scope	Does the record identify the correct customer, system, user, asset, or service?

Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Playbook L - Change and Exception Governance

Claim: security-relevant changes and deviations are authorized, tested, time-bounded where appropriate, and verified.

Primary evidence pattern:

- Change request
- Risk/security impact
- Approvals
- Implementation record
- Testing/rollback plan
- Verification
- Exception/risk acceptance
- Expiration/review date
- Closure evidence

Validation: select a normal change, an emergency change, and an active exception. Confirm that the effective environment matches the approved decision and that expired exceptions cannot persist silently.

Evidence question	**Practical check**
Scope	Does the record identify the correct customer, system, user, asset, or service?
Time	Does it show the relevant event date and evaluated period?
Authority	Can the organization show who approved or owned the action?
Effective state	Is there system-generated proof of the technical

	outcome?
Exceptions	Are deviations visible, approved, monitored, and time-bounded where appropriate?
Reproducibility	Can another authorized person locate or regenerate the evidence?

Evidence Request Record

Use one record for every formal or mock-assessment evidence request so the organization can trace what was requested and exactly what was released.

Field	Record
Request ID and date	_____
Requirement/objective	_____
Request description	_____
Owner	_____
Source system	_____
Customer/tenant	_____
Covered period	_____
Sensitivity	_____
Reviewer/approver	_____
Artifact/version released	_____
Release date	_____
Open questions/follow-up	_____

Evidence Note Template

Use an evidence note when an artifact needs concise context. The note should explain, not replace, the source evidence.

Field	Record
Artifact name/ID	_____
Claim supported	_____
Source system	_____
Tenant/system	_____

Population	_____
Date range	_____
Query/filter used	_____
What the artifact proves	_____
What it does not prove	_____
Related corroborating evidence	_____
Custodian	_____

Provider Evidence SLA Template

Use this structure when incorporating evidence obligations into managed services.

Field	Record
Artifact/report	_____
Customer-specific scope	_____
Generation frequency	_____
Historical retention	_____
Request response target	_____
Delivery method	_____
Required license/service tier	_____
Provider owner	_____
Customer archive responsibility	_____
Known limitations	_____

Evidence Health Review Template

Use a recurring evidence-health review to identify deterioration before assessment preparation.

Field	Record
Evidence source	_____
Expected cadence	_____
Last successful generation	_____

Current custodian	_____
Retrieval test result	_____
Population reconciliation result	_____
Contradictions/open issues	_____
Provider dependency	_____
Next refresh date	_____
Corrective owner	_____

Applied playbook closing: Evidence quality improves when the organization designs the operating process and the proof together. The control should work because it protects the environment; the evidence should exist because that work naturally creates traceable records. Assessment readiness then becomes an outcome of disciplined operations rather than a separate compliance production line.

CMMC for MSPs

From Readiness to Certification

Chapter 15

POA&Ms, SPRS, and Remediation

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Focus

How an MSP-supported organization turns verified deficiencies into controlled remediation, distinguishes internal corrective action from formal CMMC POA&M treatment, maintains accurate NIST and CMMC records in SPRS, and proves that closure is real, timely, and sustainable.

Chapter Contents

- Purpose, learning objectives, current source context, and terminology discipline
- 15.1–15.9 Scores, findings, status, and the difference between internal and formal remediation records
- 15.10–15.18 CMMC POA&M eligibility, prohibited deferrals, Conditional status, and the 180-day closeout clock
- 15.19–15.29 Designing, executing, validating, and governing remediation work
- 15.30–15.38 SPRS, NIST SP 800-171 DoD Assessment records, CMMC records, affirmation, and record accuracy
- 15.39–15.48 Harbor Point case studies, provider remediation, executive governance, and sustainment
- Remediation field guide, implementation checklist, workshops, review questions, key terms, and official references

Chapter Purpose

Chapter 14 established the evidence discipline needed to prove that controls work. Chapter 15 addresses the condition every organization eventually encounters: the evidence shows that something is not fully implemented, not fully supported, or no longer operating as intended. The challenge is not merely to write the deficiency into a spreadsheet. The challenge is to determine what kind of record is appropriate, what the governing rule permits, what must be corrected before an assessment can be considered final, what belongs in SPRS, and how the organization proves that the corrective action actually changed the operating environment.

For an MSP-supported organization, this work is distributed. Harbor Point Engineering may own the contractual obligation and business decision. NorthStar may implement the technical correction. Beacon Security Operations may tune monitoring and validate detection. A cloud provider may have to change a service tier or produce an artifact. A software vendor may control the patch that resolves the root cause. The remediation program therefore has to connect governance, technical execution, provider dependencies, evidence, schedule, cost, and assessment status without allowing responsibility to disappear between organizations.

This chapter also resolves a common source of confusion: not every open security item is a CMMC POA&M item, and not every score stored in SPRS is a CMMC score. Organizations should maintain a broad internal corrective-action process for all known weaknesses, while applying formal CMMC POA&M treatment only when the rule permits it. Similarly, the NIST SP 800-171 DoD Assessment results associated with DFARS 252.204-7019 and 252.204-7020 are distinct from CMMC assessment and affirmation records, even though SPRS supports both types of cyber records.

Learning Objectives

- Distinguish findings, corrective actions, operational plans of action, formal CMMC POA&Ms, and assessment closeout records.
- Explain the relationship among NIST SP 800-171 DoD Basic Assessments, SPRS summary-level scores, CMMC assessment results, Conditional status, Final status, and annual affirmation.
- Apply the Level 1 rule that POA&Ms are not permitted and the Level 2 restrictions that limit which NOT MET requirements may remain on a formal POA&M.

- Explain the 180-day closeout requirement for a Conditional CMMC status and the different closeout paths for Level 2 self-assessment and Level 2 certification assessment.
- Build remediation work packages with owners, dependencies, milestones, evidence, risk treatment, rollback, and defined closure criteria.
- Prevent score-chasing from replacing security engineering and prevent ticket closure from being mistaken for requirement closure.
- Maintain accurate, current SPRS records and separate NIST SP 800-171 DoD Assessment records from CMMC status and affirmation records.
- Coordinate MSP, MSSP, cloud, software-vendor, customer, C3PAO, and management actions without creating shared-responsibility ambiguity.
- Use re-testing, evidence reconciliation, management review, and sustainment checks to demonstrate durable remediation.

Current Source Context and Important Distinctions

This chapter is written against the CMMC Program rule in 32 CFR Part 170 and the Level 2 baseline based on NIST SP 800-171 Revision 2. Section 170.21 governs formal CMMC POA&M use and closeout. Level 1 does not permit POA&M treatment. For Level 2, Conditional status is available only when the assessment satisfies the score and eligibility conditions in the rule; certain security requirements cannot be placed on the formal POA&M. A POA&M closeout assessment must confirm closure within 180 days of the Conditional CMMC Status Date or the Conditional status expires.

Separately, DFARS 252.204-7019 and 252.204-7020 require applicable contractors to have a current NIST SP 800-171 DoD Assessment and use SPRS for summary-level assessment information. A Basic Assessment is a contractor self-assessment under the DoD Assessment Methodology and carries a Low confidence level. SPRS also supports CMMC cyber records, including Level 1 and Level 2 self-assessment entry and CMMC affirmation workflows. The presence of both record families in SPRS is operationally convenient, but it does not make them interchangeable.

Terminology Discipline

In this chapter, “internal corrective-action register” means the organization’s broad tracking mechanism for weaknesses and improvements. “Formal CMMC POA&M” means a plan used only under the conditions permitted by 32 CFR Part 170. “SPRS score” is used only when the specific record type is identified. This prevents ordinary remediation language from being mistaken for a regulatory status.

15.1 Begin With the Finding, Not the Score

A team that starts with “How many points do we need?” can miss the actual security condition. The finding should state the requirement or objective, affected scope, observed condition, evidence, and consequence before anyone discusses scoring.

Harbor Point records a failed privileged-access review as an access-governance problem first. The score is recorded because assessment rules require it, but the remediation begins with the population of privileged accounts, approval model, stale access, and review cadence.

In the context of assessment discipline, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

For MSP-supported environments, shared responsibility must be translated into specific service actions. The customer retains accountability for its contractual and CMMC representations, while the MSP or MSSP is accountable for the functions it has accepted. If a provider cannot perform a required action or produce the necessary evidence within the closeout schedule, that limitation is treated as a remediation dependency and escalated early rather than discovered during formal validation.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.2 Separate Implementation Gaps From Evidence Gaps

An implementation gap means the required protection is not operating as required. An evidence gap means the organization may be performing the activity but cannot produce sufficient reliable proof. The correction path differs.

NorthStar does not install a second technical control merely because a report is missing. It determines whether the control failed, whether the record-generation process failed, or whether the evidence was retained in a provider system that Harbor Point cannot retrieve.

In the context of assessment discipline, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.3 Use an Internal Corrective-Action Register for Every Material Weakness

The internal corrective-action register should be broader than any formal assessment POA&M. It can track architecture debt, recurring operational weaknesses, evidence failures, contract gaps, provider dependencies, training needs, and improvement work.

This broader register allows Harbor Point to manage items that are important even when they are not eligible for CMMC POA&M treatment. It also prevents teams from ignoring a weakness simply because it does not affect the current formal score.

In the context of governance, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.4 Do Not Call Every Open Item a POA&M

The word POA&M carries regulatory meaning in CMMC. Using it casually for every project plan creates confusion about eligibility, deadlines, assessment status, and customer representations.

NorthStar uses “corrective action,” “engineering backlog,” or “remediation work package” for ordinary security work. The label “CMMC POA&M” is reserved for the formal record created under the applicable CMMC rule.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.5 Understand the NIST SP 800-171 DoD Assessment Score

The DoD NIST SP 800-171 Assessment Methodology produces a summary-level score based on implementation of the 110 Revision 2 requirements. The maximum is 110, and deductions reflect the weighted values assigned by the methodology.

A Basic Assessment is self-generated and therefore has a Low confidence level under DFARS 252.204-7020. The score can support acquisition decisions, but it should not be represented as a CMMC certification result.

In the context of scoring and records, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.6 Understand What SPRS Stores and Why Record Type Matters

SPRS supports multiple cyber-report functions, including NIST SP 800-171 Assessment results and CMMC records. The user must understand which record is being viewed, entered, edited, or affirmed.

Harbor Point's compliance lead keeps a record map showing the system/security-plan identifier, CAGE codes, assessment type, date, score or status, affirming official, and supporting evidence for each government cyber record.

In the context of scoring and records, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.7 Keep CMMC Status Separate From Internal Readiness Metrics

Internal readiness percentages, dashboard colors, and project completion figures are management tools. They are not official CMMC status unless produced through the governing assessment and reporting process.

Executives may see "86% remediation complete," but Harbor Point labels that metric as internal project progress. It never substitutes that number for a CMMC assessment score or an SPRS record.

In the context of scoring and records, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a

common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.8 Preserve the Original Finding and Assessment Baseline

The organization should preserve the original finding, evidence, assessment date, and scope even after the condition is corrected. This creates traceability between what was observed and what was changed.

Replacing the original screenshot or editing the finding until it looks resolved destroys useful history. Harbor Point instead adds corrective actions, validation evidence, closure date, and approver while retaining the baseline.

In the context of evidence integrity, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.9 Establish Remediation Governance Before Work Starts

Before engineers begin work, management should define decision authority, risk ownership, funding authority, change windows, provider contacts, validation roles, and escalation paths.

Without this structure, a seemingly simple fix can stall because Harbor Point, NorthStar, Beacon, and a cloud provider each believe another party must approve the change.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.10 Level 1 Does Not Permit a CMMC POA&M

CMMC Level 1 requires all applicable safeguards to be satisfied for the relevant status; the program does not allow a formal CMMC POA&M for Level 1.

An MSP should therefore avoid promising a customer that unresolved Level 1 safeguards can be placed on a CMMC POA&M after the assessment. Internal remediation tracking can still be used before assessment, but it is not a substitute for meeting the required safeguards.

In the context of formal POA&M rules, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.11 Level 2 Conditional Status Is Limited, Not Automatic

Conditional Level 2 status is a constrained outcome available only when the assessment satisfies the rule’s conditions. It is not an entitlement and it is not a planning target that allows an organization to postpone difficult controls.

Harbor Point plans for Final status and treats Conditional status as an exception path. This changes project behavior: difficult identity, physical, encryption, and SSP issues are addressed early rather than intentionally left for the end.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.12 Apply the Formal POA&M Eligibility Rules

Formal POA&M eligibility must be checked against the current rule and the exact assessment results. The team should never decide eligibility from memory, a consultant slide, or an old checklist.

The compliance lead records the rule citation and assessment finding associated with every proposed formal POA&M item. If eligibility is uncertain, the item remains an internal corrective action until the authorized assessment process determines its treatment.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.13 Recognize Requirements That Cannot Be Deferred

The CMMC rule identifies security requirements that cannot be included on a Level 2 POA&M, and it limits treatment of certain high-value requirements. These restrictions reflect the program’s decision that some protections must already be substantially in place.

Harbor Point maintains a “must-be-MET” watch list during readiness so those requirements receive earlier technical and management attention. The list is verified against the current rule before each assessment cycle.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.14 Treat the 180-Day Clock as a Hard Program Constraint

Once Conditional status begins, the 180-day closeout period is a hard program constraint. A long procurement cycle, vendor delay, budget dispute, maintenance blackout, or staffing shortage does not extend the rule by itself.

NorthStar back-plans from the closeout deadline, reserving change windows and validation time. Harbor Point also sets an internal completion target well before day 180 so failed tests and provider delays can be corrected.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.15 Plan the POA&M Closeout Assessment From Day One

A formal POA&M should be written with closeout in mind. Each item needs a target state, implementation milestones, owner, dependency, expected evidence, test method, and date that allows enough time for the required closeout assessment.

The closeout assessor will evaluate whether the previously NOT MET requirement is now MET. A vague milestone such as “deploy security improvements” does not define what evidence must exist or how success will be demonstrated.

In the context of closeout planning, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.16 Distinguish Self-Assessment Closeout From C3PAO Closeout

For a Level 2 self-assessment, the OSA performs the POA&M closeout self-assessment in the same manner as the initial self-assessment. For a Level 2 certification assessment, an authorized or accredited C3PAO performs the closeout certification assessment.

Harbor Point does not schedule internal validation as though it were the formal C3PAO closeout. Internal testing prepares the environment; the required external closeout path remains separate when certification assessment applies.

In the context of closeout planning, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.17 Use the Re-Evaluation Window Carefully

The CMMC assessment process permits limited re-evaluation of a NOT MET requirement when additional evidence becomes available under the conditions specified by the rule. Re-evaluation is not a mechanism to redesign the environment after the assessment and pretend the original condition never existed.

Harbor Point uses the window to resolve factual or evidence issues that can be supported by valid additional evidence without undermining previously assessed results. Material remediation is handled through the proper corrective path.

In the context of assessment procedure, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a

common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.18 Avoid Designing the Program Around Conditional Status

An organization that intentionally plans to enter assessment with known eligible deficiencies is accepting schedule, contract, resource, and closeout risk. Conditional status should therefore be treated as a constrained contingency, not the default project plan.

NorthStar's readiness gate requires executive approval before an assessment proceeds with any known NOT MET condition. The decision package identifies eligibility, consequence, remediation plan, provider dependency, and closeout schedule.

In the context of program strategy, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

assessment finding; applicable rule/eligibility determination; formal POA&M record when permitted; milestone plan; closeout evidence; closeout assessment result

15.19 Convert Each Finding Into a Defined Target State

A target state should describe observable security behavior, not a product purchase. "Deploy MFA" is incomplete if the finding concerns privileged, remote, and general-user authentication paths.

Harbor Point defines which identities, applications, administrative interfaces, remote paths, exceptions, and evidence sources must show the corrected behavior.

In the context of remediation engineering, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.20 Perform Root-Cause Analysis Before Selecting the Fix

Root-cause analysis asks why the condition existed. The root cause may be technical, procedural, contractual, architectural, staffing-related, or caused by ambiguous responsibility.

If terminated users repeatedly retain cloud access, disabling one account is a correction but not a root-cause fix. The real problem may be the termination trigger, incomplete system inventory, missing provider notification, or a runbook that covers only on-premises accounts.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.21 Build Remediation Work Packages Around Outcomes

A work package groups the tasks needed to achieve one defined security outcome. It includes implementation, documentation, testing, training, provider action, evidence, and sustainment tasks rather than scattering them across unrelated tickets.

Harbor Point's "Privileged Access Correction" package contains identity cleanup, role redesign, approval workflow, monitoring changes, ticket updates, administrator training, SSP update, evidence export, and re-test.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.22 Sequence Work by Risk, Dependency, and Validation Needs

Remediation order should reflect security significance, breadth, dependencies, lead time, assessment consequences, operational risk, and validation effort. Easy tasks should not automatically be done first.

Identity, asset inventory, remote administration, encryption architecture, and provider contracts often have high dependency value because later controls and evidence rely on them.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.23 Assign One Accountable Outcome Owner

Multiple teams can perform work, but one role should own the outcome through validated closure. Otherwise each party can complete its ticket while the finding remains unresolved.

Harbor Point assigns the customer security lead as outcome owner for a shared remote-access finding even though NorthStar changes the configuration and Beacon validates monitoring.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.24 Make MSP and Provider Dependencies Explicit

Provider dependencies should be tracked as explicit milestones with named contacts, requested artifacts, response dates, and escalation paths. “Waiting on vendor” is not a remediation strategy.

NorthStar identifies which dependencies require a cloud-provider feature, a software patch, a licensing change, or an MSSP detection update and escalates them before they threaten the closeout schedule.

In the context of provider management, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.25 Integrate Change Control, Testing, and Rollback

Security remediation can create outages or weaken other controls if rushed. Every production change should define approvals, maintenance windows, pre-checks, rollback, post-change validation, and monitoring.

A firewall correction that blocks unauthorized traffic but also breaks backup replication can create a new availability and recovery problem. Harbor Point therefore validates both the intended control outcome and critical dependent services.

In the context of change management, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete

while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.26 Define Closure Evidence Before Implementation

Closure evidence should be defined before work starts. This keeps implementation focused on the requirement and prevents the team from discovering after the change that it cannot demonstrate the corrected state.

For a vulnerability-management finding, closure evidence may include updated inventory reconciliation, current scan results, exception records, patch/deployment evidence, re-scan results, and the operating procedure that sustains the process.

In the context of evidence planning, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.27 Re-Test the Requirement, Not Merely the Ticket

A closed service ticket proves that work was recorded as complete; it does not prove the security requirement is MET. Re-testing should evaluate the same population, workflow, or technical behavior described by the original finding.

NorthStar re-runs the relevant query, samples affected systems, confirms no unintended exceptions, and produces customer-specific evidence. Harbor Point then reviews the result against the requirement and objective.

In the context of validation, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.28 Update the SSP, Diagrams, Inventories, and Responsibility Matrix

Remediation changes the system description. The SSP, network and data-flow diagrams, asset inventory, service inventory, responsibility matrix, procedures, and evidence index should be reconciled as part of closure.

A technical fix that leaves documentation describing the old architecture creates future assessment and operational risk. Documentation is therefore part of the work package, not a later cleanup project.

In the context of documentation, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.29 Prevent Reopened Findings Through Sustainment Controls

The corrected condition should have an owner, monitoring method, review cadence, exception process, and trigger for re-evaluation. Otherwise the finding may return as soon as project attention moves elsewhere.

Harbor Point adds recurring privileged-access review and evidence-health checks after closing an access finding, turning a one-time fix into a sustained control.

In the context of sustainment, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.30 Understand SPRS as a Government Cyber-Record System

SPRS is an authoritative DoD system used for supplier and cyber-related records, including NIST SP 800-171 Assessment results and CMMC records. Vendors should use current SPRS guides and role-based access procedures.

The organization should treat record entry as a controlled business process because inaccurate CAGE, scope, score, date, or affirmation information can affect acquisition decisions and internal representations.

In the context of SPRS operations, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.31 Maintain Accurate NIST SP 800-171 DoD Assessment Records

For applicable DFARS requirements, the contractor should ensure current NIST SP 800-171 DoD Assessment summary-level scores exist for relevant covered contractor information systems. The underlying assessment record should identify the SSP/system context and assessment date.

Harbor Point maintains a source worksheet showing the assessment methodology used, score calculation, SSP version, CAGE associations, assessment date, and responsible preparer so later staff can reconstruct the basis for the SPRS record.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.32 Maintain Accurate CMMC Self-Assessment Records

CMMC Level 1 and applicable Level 2 self-assessment records follow CMMC procedures rather than the older NIST Basic Assessment workflow. The organization should use the current SPRS CMMC entry guidance and verify the exact assessment scope and status being recorded.

NorthStar may provide evidence and technical assistance, but Harbor Point controls the organization’s official representation unless authority is explicitly and lawfully assigned.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.33 Manage the Affirming Official Workflow

The Affirming Official is a senior representative with responsibility and authority to affirm continuing compliance. Affirmation should therefore be supported by a management review, not treated as a clerical click.

Harbor Point's AO receives a concise package summarizing assessment status, scope, material changes, open risks, provider changes, unresolved exceptions, and evidence-health results before affirming.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.34 Reconcile CAGE, System, and Scope Identifiers

Government cyber records depend on accurate organizational and system identifiers. CAGE hierarchies, system names, SSP versions, assessment scopes, and provider relationships should be reconciled before entry or affirmation.

A technically accurate assessment tied to the wrong CAGE or an outdated system description can create visibility and eligibility problems. Harbor Point adds identifier reconciliation to its pre-submission checklist.

In the context of record identity, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.35 Control Who Can Enter, Edit, and Affirm Cyber Records

Access to SPRS and related cyber reporting functions should follow least privilege and separation of duties. The person preparing source data does not necessarily need authority to affirm compliance.

Harbor Point documents who may prepare, enter, review, approve, and affirm records, and maintains backup personnel so a deadline is not missed because one account holder is unavailable.

In the context of access governance, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.36 Preserve the Evidence Behind Submitted Records

Every submitted score, status, or affirmation should have a retrievable evidence package supporting the representation. This is not merely for assessment convenience; it protects management from relying on a number whose basis can no longer be explained.

The package preserves the assessment date, scope, SSP version, findings, score worksheet when applicable, corrective actions, closure evidence, and management approval.

In the context of evidence integrity, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete

while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.37 Correct Record Errors Without Hiding Historical Facts

If a record error is discovered, the organization should correct it through the appropriate process while preserving internal traceability. It should not silently rewrite supporting documents to make the history appear different.

Harbor Point records what was wrong, when it was discovered, who authorized the correction, what official record was changed, and whether any contracting or management stakeholders need notification.

In the context of record correction, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.38 Build an SPRS Readiness Runbook

An SPRS runbook should describe account prerequisites, roles, record types, source data, review steps, screenshots or references to current system guidance, approval, affirmation, and evidence retention.

Because interfaces and program procedures can change, Harbor Point dates the runbook and requires a current-guide check before every significant submission.

In the context of operational readiness, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

record-type map; system/SSP and CAGE identifiers; assessment date; source score or status; access/approval evidence; affirmation or correction record; retained support package

15.39 Harbor Point Case: The Score Is Not the Remediation Plan

Harbor Point’s readiness review finds six open issues. Management initially asks which combination preserves the highest score. The security lead redirects the meeting to affected requirements, business impact, eligibility, root cause, dependencies, and closure evidence.

The exercise demonstrates that score awareness is necessary, but score optimization is not a substitute for security engineering. Two lower-point findings can still expose critical workflows, while one high-value deficiency may represent a broader architectural weakness.

In the context of case study, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.40 Harbor Point Case: A Finding That Cannot Simply Be Deferred

A proposed formal POA&M item involves a requirement that the rule does not permit to be deferred. The team cannot make the item eligible by relabeling it, splitting it into smaller tasks, or calling the issue “documentation.”

Harbor Point pauses assessment scheduling, completes the correction, and validates it before proceeding. The internal project plan remains useful, but it is not represented as a CMMC POA&M.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.41 Harbor Point Case: Conditional Level 2 Closeout

Harbor Point receives Conditional Level 2 status with a small number of eligible NOT MET requirements. The closeout plan begins immediately, with internal completion targeted well before the 180-day deadline.

NorthStar completes technical work, Beacon validates monitoring changes, Harbor Point updates the SSP and evidence package, and the appropriate closeout assessment confirms the previously NOT MET requirements are now MET.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.42 Harbor Point Case: Provider Evidence Blocks Closure

A technical control is operating, but the external provider cannot produce customer-specific historical evidence needed for closeout. The weakness is therefore partly contractual and operational, not merely technical.

Harbor Point escalates the evidence obligation, obtains a provider export, changes the service agreement, and creates a recurring evidence-delivery process so the same dependency does not block future assessment activity.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.43 Harbor Point Case: The Vulnerability Was Patched but the Requirement Was Not Closed

NorthStar patches every server listed in the original vulnerability report and closes the ticket. Re-testing finds two in-scope servers absent from the scanner and one unsupported appliance with the same exposure.

The finding remains open because the requirement concerns flaw remediation across the relevant population, not only installation success on the devices that happened to appear in the first report. Inventory reconciliation and exception handling become part of closure.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.44 Build an Executive Remediation Dashboard

Executives need a view that supports decisions without hiding uncertainty. The dashboard should show open findings, formal POA&M items if any, must-be-MET blockers, days remaining to closeout, overdue dependencies, validation status, spend, and residual risk.

Harbor Point separates official CMMC status from internal project indicators and labels each date and metric clearly.

In the context of executive governance, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.45 Budget for One-Time Correction and Recurring Sustainment

A correction can create permanent operating cost: additional licensing, recurring evidence exports, after-hours monitoring, periodic reviews, specialist support, or new audit storage.

Budgeting only for implementation can recreate the gap when the temporary project funding ends. NorthStar prices recurring service duties before closure so the control can remain sustainable.

In the context of financial planning, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.46 Use Metrics That Reward Durable Closure

Useful metrics measure time to validate, repeat-finding rate, age of unresolved high-impact items, provider dependency aging, percentage of closure tests passed on first attempt, and recurrence after closure.

Ticket counts and raw percent complete can encourage superficial closure. Harbor Point therefore measures whether the corrected condition remains healthy over subsequent review cycles.

In the context of metrics, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a

single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.47 Perform a Post-Closeout Integrity Review

After formal closeout, the organization should verify that all related documents, evidence repositories, dashboards, government records, provider obligations, and monitoring processes reflect the final state.

This integrity review catches contradictions such as an SSP still describing the old control, a dashboard still showing the item open, or a provider contract that never incorporated the recurring duty.

In the context of validation, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

15.48 Operate a Continuous Remediation and Readiness Cycle

Continuous readiness treats new deficiencies as normal inputs to governance rather than emergencies reserved for assessment season. Findings enter one controlled

process, receive ownership and priority, are corrected, validated, documented, and monitored for recurrence.

For an MSP, this model turns CMMC remediation into part of ordinary service management. The result is not a permanently perfect environment; it is an environment in which drift and weakness are found early, decisions are explicit, and closure can be demonstrated.

In the context of sustainment, the practical management question is whether the organization can connect the observed condition to a responsible owner, a defined correction, a realistic schedule, and objective closure evidence. Harbor Point uses a single traceable record that links the original finding to change tickets, provider actions, test results, document updates, and management decisions. This prevents a common failure mode in which each team can show that its local task is complete while no one can demonstrate that the security outcome is complete across the assessment scope.

Evidence to Preserve

finding baseline; owner and decision record; implementation/change records; validation output; updated documentation; closure approval

Remediation Field Guide for MSP-Supported Organizations

The field guide below converts the chapter into a working operating model. It is intentionally broader than formal CMMC POA&M management because most organizations need to manage security weaknesses continuously, not only when an assessment produces Conditional status.

Situation	Immediate Action	Record	Closure Test
New readiness finding	Confirm scope, requirement, evidence, and owner	Internal corrective-action register	Re-test affected objective and population
Potential formal CMMC POA&M item	Verify current rule eligibility and assessment conditions	Formal POA&M only if permitted	Required POA&M closeout assessment
Level 1 NOT MET safeguard	Remediate before achieving required Level 1 status	Internal remediation record	Reassess safeguard; no CMMC POA&M path
Provider dependency	Assign provider contact, due date, escalation, alternate path	Dependency/milestone record	Customer-specific result and evidence received

Patch installed	Do not close automatically	Change ticket + vulnerability record	Re-scan/reconcile full in-scope population
SPRS record due	Identify exact record type and source package	Submission/affirmation checklist	Second-person review against source data
Record error discovered	Preserve history and correct through proper process	Correction log	Official record reconciled to evidence
Conditional status	Back-plan from 180-day closeout requirement	Formal milestone schedule	Closeout completed and final status confirmed

Chapter 15 Implementation Checklist

- Use one internal corrective-action register for all material security weaknesses, regardless of formal POA&M eligibility.
- Do not label ordinary backlog items as CMMC POA&Ms.
- Retain the original finding, assessment date, scope, and evidence baseline.
- Separate implementation gaps, evidence gaps, documentation gaps, scope gaps, and provider gaps.
- Identify the exact assessment or record type before discussing a score.
- Confirm current formal POA&M eligibility from the governing rule and assessment process.
- Remember that Level 1 does not permit a CMMC POA&M.
- Flag requirements that cannot be placed on a Level 2 POA&M and address them early.
- Back-plan every Conditional-status remediation from the 180-day closeout deadline.
- Set an internal completion target earlier than the regulatory closeout deadline.
- Define target state and closure evidence before implementation begins.
- Perform root-cause analysis for recurring or systemic findings.
- Group related tasks into outcome-based work packages.
- Assign one accountable outcome owner even when several organizations perform work.
- Track MSP, MSSP, CSP, software-vendor, and customer dependencies explicitly.
- Use change control, pre-checks, rollback, post-change validation, and enhanced monitoring.
- Re-test the requirement and affected population rather than relying on ticket closure.

- Update SSP, diagrams, inventories, procedures, responsibility matrix, and evidence index during closure.
- Confirm sustainment ownership and recurring cost before marking the finding closed.
- Maintain a record map for NIST SP 800-171 DoD Assessment and CMMC records in SPRS.
- Reconcile CAGE codes, SSP/system identifiers, scope, dates, and record types before submission.
- Limit SPRS access according to role and separate preparation from affirmation where practical.
- Provide the Affirming Official with a decision-quality package before affirmation.
- Retain the source evidence supporting every submitted score, status, and affirmation.
- Correct official record errors transparently and retain internal correction history.
- Use executive dashboards that separate official status from internal project metrics.
- Measure repeat findings, validation quality, dependency aging, and sustained health—not just ticket volume.
- Perform a post-closeout integrity review across technical, documentary, provider, and government records.
- Incorporate lessons learned into service design, staffing, contracts, automation, and recurring reviews.
- Review current official CMMC, DFARS, and SPRS guidance before relying on dates, workflows, or eligibility rules.

Operational Workshops

Workshop 1 - Classify the Finding

Given ten sample findings, classify each as implementation, evidence, documentation, scope, or provider-related. Decide which belong in the internal register and which could potentially require formal assessment treatment.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 2 - POA&M Eligibility Review

Take five NOT MET Level 2 findings and build an eligibility worksheet. Identify score effect, rule restrictions, whether the item can remain on a formal POA&M, and what must be MET before Conditional status is possible.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 3 - 180-Day Back-Plan

Create a closeout calendar beginning at the Conditional status date. Include procurement, provider lead time, implementation, rollback window, internal testing, evidence refresh, document updates, management review, and formal closeout assessment.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 4 - Root Cause vs. Symptom

Analyze repeated stale-account findings. Trace triggers from HR to customer approval to MSP execution to SaaS account closure to validation. Identify which change prevents recurrence.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 5 - Closure Evidence Design

For a vulnerability-management finding, define the exact evidence needed before work starts. Include population definition, pre-change results, deployment evidence, exception treatment, re-scan, and sustainment evidence.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 6 - SPRS Record Map

Create a table that distinguishes NIST SP 800-171 DoD Basic Assessment records, CMMC Level 1 self-assessment, CMMC Level 2 self-assessment, certification assessment visibility, and affirmation responsibilities.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 7 - Provider Dependency Escalation

Simulate a CSP that cannot provide a required historical report until after the internal closeout target. Build the escalation, alternate evidence, contract, and executive decision path.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 8 - Executive Remediation Review

Prepare a one-page decision package showing must-be-MET blockers, formal POA&M items, days to deadline, provider dependencies, cost, business disruption, and validation readiness.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 9 - Re-Test a Closed Ticket

Select a completed technical ticket and independently test whether the original requirement is now satisfied across the full in-scope population. Record any difference between task completion and requirement closure.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Workshop 10 - Post-Closeout Integrity Review

After a simulated Final status, compare SSP, diagrams, inventory, responsibility matrix, evidence index, MSP runbooks, dashboard, and government record summary. Resolve every contradiction.

- Define the starting evidence and scope.
- Identify customer and provider roles.
- Record decisions and assumptions.
- Produce objective closure criteria.
- Identify what should become a recurring operating process.

Applied Remediation Playbooks

The following playbooks provide repeatable patterns for common MSP-supported findings. They are not substitutes for the governing requirement or the facts of a specific environment. Their purpose is to show how a finding can be converted into a controlled sequence from baseline through validated closure and sustainment.

Playbook A - Identity and MFA Deficiency

Use this playbook when MFA is missing, inconsistently enforced, bypassed through legacy protocols, or not applied to all relevant privileged, remote, or user authentication paths.

70. Define every in-scope identity store, application, remote path, administrative interface, break-glass account, service account, and exception.
71. Identify whether the gap is technical enforcement, enrollment, conditional-access logic, legacy protocol exposure, exception approval, or evidence.
72. Implement the correction through controlled policy changes and staged testing.

73. Test representative privileged, remote, and general-user paths; attempt known bypass methods where safe.
74. Preserve policy exports, enrollment/population reports, exception records, test results, change approvals, and post-change monitoring.
75. Update the SSP, identity architecture, administrative runbook, and access-review evidence source.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook B - Encryption and FIPS-Validation Deficiency

Use this playbook when encryption exists but does not satisfy the required validation condition, when data paths are unclear, or when teams confuse product capability with configured use.

76. Map the exact CUI path at rest and in transit, including endpoint, server, cloud, backup, remote support, and removable-media flows.
77. Identify cryptographic modules and operating modes actually used, not merely listed in product documentation.
78. Separate “encryption present” from “required validated cryptography demonstrated.”
79. Plan upgrades, configuration changes, service-tier changes, or architecture changes with rollback and interoperability testing.
80. Capture module/version evidence, configuration, test results, provider evidence, exceptions, and change records.
81. Re-test the actual workflow and update diagrams, SSP statements, and procurement standards.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook C - System Security Plan Deficiency

Use this playbook when the SSP is missing, materially outdated, internally contradictory, or does not describe the actual assessed environment.

82. Freeze the current technical baseline long enough to identify authoritative scope, assets, locations, providers, and major control implementations.
83. Reconcile the SSP to network diagrams, data flows, inventories, cloud services, administrative paths, and the responsibility matrix.
84. Assign section owners for technical accuracy rather than allowing one compliance writer to guess operational facts.
85. Resolve contradictions explicitly; do not hide unresolved differences behind generic language.
86. Approve the revised SSP through management and establish change triggers tied to architecture and service changes.
87. Preserve review comments, approvals, source records, version history, and the date the revised SSP became authoritative.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook D - Vulnerability and Patch Closure

Use this playbook when a scanner report, patch backlog, unsupported system, or recurring vulnerability indicates that flaw remediation is incomplete.

88. Reconcile scanner coverage to the authoritative in-scope asset inventory before prioritizing individual findings.
89. Classify issues by exploitability, exposure, business importance, known exploitation, dependency, and available mitigation.
90. Define separate paths for patching, configuration mitigation, isolation, upgrade, replacement, or approved exception.
91. Deploy in controlled rings with rollback and service validation.
92. Re-scan or otherwise verify the corrected state across the full affected population.
93. Retain before/after results, exceptions, failed deployments, unsupported-asset decisions, and recurring health metrics.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook E - Logging and Monitoring Coverage Gap

Use this playbook when critical events are not collected, logs are retained too briefly, customer attribution is weak, or alerting does not create an actionable response path.

94. Define required log sources and security events by asset class and workflow.
95. Compare expected sources with actual ingestion and identify silent sources, parsing failures, time-sync problems, and tenant-mapping weaknesses.
96. Correct collection and retention before tuning alerts so detection logic is built on complete data.
97. Generate benign test events and trace them through collection, correlation, alert, case, notification, and closure.
98. Preserve source inventory, ingestion health, retention configuration, detection logic, test cases, and analyst case evidence.
99. Add recurring pipeline health tests so the same gap is detected before the next assessment.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook F - External Service Provider Dependency

Use this playbook when a required security function, evidence source, or remediation action depends on an MSP, MSSP, CSP, SaaS provider, or specialized vendor.

100. State exactly what the customer requires from the provider: technical action, evidence, notification, retention, export, testing, or contractual commitment.
101. Identify the provider owner, escalation route, contractual basis, lead time, service limitation, and alternate path.
102. Separate provider capability evidence from customer-specific implementation evidence.

103. Set milestone dates earlier than formal closeout deadlines and escalate missed dates immediately.
104. Update service descriptions, responsibility matrix, runbooks, and evidence-delivery expectations when the dependency becomes recurring.
105. Validate the customer outcome rather than accepting a generic provider attestation as closure.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook G - Physical Access and Visitor-Control Finding

Use this playbook when visitor escort, access logs, badge/key management, facility boundaries, or physical access revocation is not operating consistently.

106. Define the physical boundary and identify facilities, rooms, cabinets, media areas, and systems relevant to the assessed environment.
107. Compare authorized-access lists, badge/key inventories, visitor records, termination records, and observed physical practices.
108. Correct missing revocation, escort, logging, or access-device control through facilities and HR/MSP coordination.
109. Test the process with a sample visitor and a terminated-user scenario where appropriate.
110. Preserve access lists, logs, badge records, visitor evidence, approvals, and test observations.
111. Tie physical changes to the SSP and location/scope record.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook H - Cloud and SaaS Configuration Finding

Use this playbook when the customer relies on a cloud or SaaS service whose tenant configuration, service offering, data location, administrative model, or evidence does not match the documented design.

112. Identify the exact service offering, tenant, licensing tier, region, integrations, administrative roles, and CUI workflow.
113. Map inherited/provider responsibilities separately from customer configuration responsibilities.
114. Correct tenant settings, identity controls, logging, retention, encryption, sharing, and integrations as required.
115. Capture customer-specific exports and provider assurance applicable to the exact service.
116. Test actual user and administrative workflows, including sharing, external access, and support paths.
117. Update cloud inventory, data flows, responsibility matrix, SSP, and evidence index.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook I - Incident-Response Finding

Use this playbook when the plan exists but escalation, reporting, preservation, provider coordination, or exercises reveal that the response capability is not operational.

118. Trace one realistic incident from detection through triage, authority, containment, investigation, reporting decision, evidence preservation, recovery, and lessons learned.
119. Identify missing contacts, ambiguous decision authority, provider notification gaps, inaccessible logs, or reporting dependencies.
120. Correct the runbook and technical prerequisites, not just the policy text.
121. Conduct a tabletop or operational test with Harbor Point, NorthStar, Beacon, management, and relevant providers.

122. Preserve exercise injects, decisions, timelines, gaps, corrective actions, and evidence of completed improvements.
123. Schedule recurring exercises and validate after major architecture or provider changes.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook J - Security Training and Personnel Finding

Use this playbook when required training, role-specific instruction, onboarding, termination, or personnel security records are incomplete or inconsistent.

124. Define populations and role-based training requirements rather than relying on one global course assignment.
125. Reconcile HR population, active accounts, privileged roles, contractors, and provider personnel against training records.
126. Correct missed assignments and the trigger/process that allowed people to escape the requirement.
127. For MSP administrators, include customer-specific handling, remote support, evidence, incident, and escalation responsibilities.
128. Preserve completion records, curriculum/version, assignment logic, exceptions, and escalation evidence.
129. Automate recurring reconciliation where practical and include the process in onboarding/offboarding runbooks.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook K - SPRS Record Error or Mismatch

Use this playbook when the organization discovers an incorrect score, date, CAGE association, system identifier, status, affirmation, or other cyber-report information.

130. Stop downstream reuse of the suspect data and identify the exact record type and field in question.
131. Retrieve the authoritative assessment, SSP, CAGE hierarchy, source worksheet, and approval record.
132. Determine whether the error is a source-data problem, entry mistake, stale record, hierarchy issue, or misunderstanding of record type.
133. Use the current SPRS or program correction process and document who authorized the change.
134. Preserve before/after evidence and assess whether contracting, executive, assessor, or customer stakeholders require notification.
135. Update the runbook so the same control failure is caught by future second-person review.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Playbook L - Affirmation Readiness Deficiency

Use this playbook when the annual or status-related affirmation is approaching but management cannot confidently state that the assessed condition remains accurate.

136. Compare current scope, SSP, providers, architecture, privileged access, major incidents, remediation status, and evidence health to the last valid assessment baseline.
137. Identify material changes and determine whether they affect scope, requirements, assessment basis, or the truth of the planned affirmation.
138. Resolve open contradictions before asking the Affirming Official to act.
139. Prepare a concise management package with status, limitations, risks, and supporting evidence.
140. Record the review and affirmation date and preserve the basis for the official representation.
141. Use findings from the affirmation review to trigger the next continuous-readiness cycle.

Playbook Closure Standard

Do not close the playbook because every assigned task is marked complete. Close it only when the

original security outcome has been re-tested, related documentation and provider responsibilities have been reconciled, required evidence is retrievable, and recurring ownership has been assigned.

Review Questions

142. Why should remediation begin with the finding rather than the score?
143. What is the difference between an implementation gap and an evidence gap?
144. Why should the internal corrective-action register be broader than a formal CMMC POA&M?
145. Why is it risky to call every backlog item a POA&M?
146. What does a NIST SP 800-171 DoD Basic Assessment represent?
147. Why must an organization distinguish NIST assessment records from CMMC records in SPRS?
148. Why should internal readiness percentages not be represented as official CMMC status?
149. What information from the original finding should be preserved after remediation?
150. What governance decisions should be made before remediation begins?
151. What is the Level 1 rule regarding CMMC POA&Ms?
152. Why is Conditional Level 2 status not automatic?
153. How should a team determine whether a finding is eligible for formal POA&M treatment?
154. Why should must-be-MET requirements be identified early?
155. What does the 180-day closeout period change about project planning?
156. Why should closeout evidence be designed when the POA&M item is created?
157. Who performs Level 2 self-assessment POA&M closeout and who performs certification closeout?
158. What is the purpose of the limited re-evaluation window?
159. Why is planning to rely on Conditional status strategically risky?
160. What makes a remediation target state observable?
161. How does root-cause analysis differ from correcting a symptom?
162. What should an outcome-based work package include?
163. Which factors should influence remediation sequencing?
164. Why should one person or role own the remediation outcome?
165. How should provider dependencies be managed?
166. Why are change control and rollback important during security remediation?

167. Why must closure evidence be defined before implementation?
168. Why does ticket closure not prove requirement closure?
169. Which system documents should be reconciled after remediation?
170. What sustainment mechanisms reduce repeat findings?
171. What cyber record functions does SPRS support?
172. What source information should support a NIST SP 800-171 DoD Assessment record?
173. How should CMMC self-assessment records differ from generic internal assessment records?
174. What should the Affirming Official review before affirmation?
175. Why do CAGE and system identifiers matter?
176. How should access to SPRS cyber records be governed?
177. What evidence should support a submitted score or status?
178. How should an organization handle an error in an official cyber record?
179. What should an SPRS readiness runbook contain?
180. Which metrics better indicate remediation quality than ticket count?
181. What is the purpose of a post-closeout integrity review?

Answer Guidance

Questions 1 through 9 focus on remediation discipline. Begin with the verified condition, preserve the baseline, distinguish the type of gap, and create governance before work begins. Internal corrective tracking should cover all important weaknesses, while regulatory terminology should be reserved for the situations in which it actually applies.

Questions 10 through 18 focus on formal CMMC POA&M treatment. Level 1 does not permit a CMMC POA&M. Level 2 Conditional status depends on the rule's scoring and eligibility conditions, certain requirements cannot be deferred, and the closeout assessment must be completed within the 180-day period. Internal readiness work prepares for the formal process but does not replace it.

Questions 19 through 29 focus on remediation engineering and sustainment. Target states should be observable, work packages should include technical and nontechnical dependencies, closure criteria should be defined before implementation, and validation should test the original requirement across the relevant population. Documentation and recurring operations must be updated as part of closure.

Questions 30 through 40 focus on SPRS, affirmation, and integrity. Determine the exact record type, reconcile identifiers, preserve source evidence, apply least privilege, support the Affirming Official with a management-quality review, correct errors transparently, and validate that all records agree after closeout.

Key Terms

Term	Working Meaning
Corrective-action register	Internal tracking record for weaknesses, remediation, improvements, and dependencies regardless of formal CMMC POA&M eligibility.
Formal CMMC POA&M	A Plan of Action and Milestones used only when permitted by the CMMC rule for a qualifying assessment outcome.
Conditional CMMC Status	Time-limited status available when the applicable assessment meets the rule's conditions and eligible NOT MET requirements are placed on an allowed POA&M.
Final CMMC Status	Status achieved when the applicable assessment requirements are fully satisfied, including successful POA&M closeout when Conditional status was used.
POA&M closeout assessment	Assessment limited to the NOT MET requirements identified on the formal POA&M and used to confirm they have been remediated.
NIST SP 800-171 DoD Basic Assessment	Contractor self-assessment conducted under the DoD Assessment Methodology and associated with a Low confidence level.
SPRS	Supplier Performance Risk System, a DoD system supporting supplier performance information and cyber records including NIST assessment and CMMC functions.
Affirming Official	Senior organizational representative responsible for affirming continuing compliance under the CMMC Program.
Target state	Observable condition that defines what successful remediation must accomplish.
Closure evidence	Objective evidence demonstrating that the finding has been corrected and the requirement now operates as intended.
Root cause	Underlying process, architecture, responsibility, resource, contractual, or technical condition that produced the finding.
Outcome owner	Role accountable for moving a remediation item from finding through validated and sustainable closure.
Dependency	Required action, decision, provider response, resource, or technical condition that must occur before a

	remediation outcome can be completed.
Re-test	Validation activity that re-evaluates the affected requirement, objective, population, or workflow after corrective action.
Sustainment	Recurring ownership, monitoring, review, funding, and evidence generation that keep a corrected control operating over time.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification Program. See especially sections governing Level 1 and Level 2 assessment, affirmation, scoring, POA&M requirements, and closeout.

R2. 32 CFR 170.21, Plan of Action and Milestones requirements. Formal CMMC POA&M use is limited by level, score, eligibility conditions, and prohibited requirements; closeout must be confirmed within 180 days of the Conditional CMMC Status Date.

R3. Defense Federal Acquisition Regulation Supplement 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements, and 252.204-7020, NIST SP 800-171 DoD Assessment Requirements. These provisions address current NIST SP 800-171 DoD Assessments and SPRS summary-level scores for applicable covered contractor information systems.

R4. Department of Defense NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 (June 24, 2020), or the current applicable version referenced by DFARS. Use for Basic, Medium, and High Assessment scoring and confidence context.

R5. Supplier Performance Risk System (SPRS) Cyber Reports resources, CMMC quick-entry guides, tutorials, vendor access instructions, and FAQs. Use current SPRS guidance for record entry, editing, affirmation, CAGE hierarchy, and access procedures.

R6. Department of Defense CMMC documentation, Level 1 and Level 2 assessment/scoping guides, FAQs, and current program announcements. Verify current program implementation status before relying on transition dates or acquisition timing.

R7. National Institute of Standards and Technology SP 800-171 Revision 2 and NIST SP 800-171A (June 2018) as incorporated by the CMMC Program rule for the Level 2 baseline and assessment procedure discussed in this chapter.

R8. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, and the organization’s actual solicitation, contract, task order, and subcontract clauses. Remediation and assessment records do not replace the underlying safeguarding obligation.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance for readiness, remediation, and record-management work. It does not replace the governing regulation, the applicable solicitation or contract, current DoD/SPRS guidance, legal advice, or an authorized CMMC assessment determination.

Chapter Closing

A mature remediation program does not use a POA&M as a parking lot and does not use SPRS as a place to store numbers that no one can later explain. It starts with accurate findings, assigns ownership, corrects root causes, validates the full security outcome, updates the system record, and sustains the corrected condition. Formal CMMC POA&M treatment is then one carefully bounded part of a much larger security-management discipline.

For Harbor Point and NorthStar, the most important lesson is that the score, the ticket, the POA&M, the SPRS record, and the final status are related but not interchangeable. The score summarizes an assessment. The ticket records work. The POA&M controls eligible deferred deficiencies under a specific rule. SPRS preserves government-facing records. Final closure requires the security requirement itself to be demonstrably satisfied. Keeping those concepts separate makes the entire program more accurate and more defensible.

The next stage of the book builds on this foundation by examining how an MSP can maintain readiness after the immediate remediation cycle: managing changes, recurring assessments, provider evolution, contract changes, personnel turnover, and the continuous evidence needed to keep a previously valid security posture from silently drifting out of alignment.

CMMC for MSPs

From Readiness to Certification

Chapter 16

Continuous Compliance and Maintaining CMMC Readiness

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Focus

How an MSP-supported organization converts CMMC readiness from a project into a durable operating condition by monitoring control health, managing change, preserving evidence, maintaining accurate scope and provider responsibilities, completing annual affirmation activities, and preparing continuously for the next assessment cycle.

Chapter Contents

- Purpose, learning objectives, current source context, and the continuous-readiness operating model
- 16.1–16.9 Sustained compliance, governance, ownership, and readiness baselines
- 16.10–16.18 Continuous control monitoring, evidence health, metrics, and review cadence
- 16.19–16.28 Change management, scope drift, provider changes, technology lifecycle, and exceptions
- 16.29–16.38 Annual affirmation, SPRS/CMMC records, subcontractors, contracts, and executive oversight
- 16.39–16.48 Harbor Point case studies, readiness exercises, next-cycle planning, and the MSP operating model
- Continuous-readiness field guide, implementation checklist, workshops, review questions, key terms, templates, and official references

Chapter Purpose

Chapter 15 focused on deficiencies: how to classify them, remediate them, manage formal POA&M limits, maintain accurate SPRS records, and prove closure. Chapter 16 addresses what happens after the urgent corrective work is finished. The environment continues to change. People join and leave. Cloud services add features. Firewall rules accumulate. MSP tooling changes. Subcontractors are replaced. Vulnerabilities are published. Business units adopt new applications. Contracts change. If the organization treats CMMC readiness as a completed project, the condition that was assessed can begin drifting almost immediately.

Continuous compliance does not mean that every control is watched every second or that nothing is ever allowed to change. It means the organization has a management system that detects important change, assigns ownership, evaluates security and scope consequences, preserves evidence, corrects drift, and keeps official representations aligned with the environment that actually exists. For an MSP-supported organization, that management system must reach across customer personnel, MSP administrators, MSSP analysts, cloud providers, subcontractors, and business owners. A control can fail because any one of those participants stops performing its part.

This chapter develops a practical continuous-readiness operating model around Harbor Point Engineering, NorthStar Managed Technology, and Beacon Security Operations. The emphasis is not on generating more compliance meetings. It is on embedding CMMC-relevant checks into the work already required to run a secure environment: onboarding, termination, patching, vulnerability remediation, change approval, incident response, provider governance, backup testing, evidence review, architecture decisions, contract review, and management reporting.

The central principle is that readiness should be observable on an ordinary operating day. If management needs three weeks to reconstruct asset inventories, privileged access, provider responsibilities, logging coverage, or evidence history before an assessment, the organization does not have continuous readiness. It has periodic reconstruction. The objective of this chapter is to replace reconstruction with sustained control.

Learning Objectives

- Explain continuous compliance as an operating discipline rather than a permanent claim that nothing can change.
- Design recurring governance and review cadences that match control risk, evidence generation, provider dependencies, and business change.

- Use control-health indicators and exception records to detect drift before it becomes an assessment finding or operational incident.
- Maintain current scope, asset, information-flow, SSP, responsibility-matrix, and provider records as the environment changes.
- Integrate CMMC impact analysis into change management, procurement, cloud adoption, mergers, office moves, and service transitions.
- Maintain evidence health by testing generation, retention, customer attribution, retrieval, and custodian continuity.
- Coordinate annual affirmations and applicable SPRS/CMMC records with management review and objective evidence.
- Monitor subcontractor and provider dependencies so flowdown, service evidence, and customer responsibilities remain accurate.
- Use metrics that reveal control health, exception aging, evidence deterioration, provider performance, and recurring root causes.
- Prepare continuously for the next assessment cycle without staging the environment or creating a parallel compliance operation.

Source Context and Current Implementation Note

This chapter uses 32 CFR Part 170, applicable DFARS clauses, the CMMC Level 2 framework based on NIST SP 800-171 Revision 2, and the assessment and affirmation concepts already discussed in earlier chapters. Where the contract includes DFARS 252.204-7021, the contractor is required to maintain the specified CMMC status for the duration of the contract, maintain annual affirmations for each applicable CMMC UID, and report applicable changes in CMMC UIDs. Those obligations make sustainment a contractual operating issue, not merely an assessment-preparation preference. [R1, R2]

As of September 2026, the Department has suspended CMMC Phase II implementation while Phase I self-assessment requirements remain in place and a broader program review proceeds. Underlying safeguarding obligations continue. Organizations should therefore confirm the current acquisition status before relying on an implementation date, while still maintaining the cybersecurity practices, assessment records, and contractual obligations that apply to their work. [R3]

Operating Principle

Continuous readiness is not the absence of change. It is the ability to change without losing control of scope, security requirements, evidence, responsibilities, and official representations.

16.1 Readiness Is a Maintained State, Not a Finish Line

Readiness Is a Maintained State, Not a Finish Line matters because continuous readiness as a maintained operating state. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

The practical challenge is drift. A procedure may still exist while the systems, people, provider services, or business assumptions underneath it have changed. NorthStar therefore compares what the documentation says should happen with what the platforms and service records show actually happened. When the two disagree, the team opens a controlled exception or corrective action rather than updating the narrative to fit the current state without investigation.

Shared responsibility makes this discipline especially important. Harbor Point retains accountability for its contractual and CMMC representations, but NorthStar or Beacon may perform the technical work and preserve much of the operational evidence. The responsibility boundary should therefore be visible in service descriptions, the Customer Responsibility Matrix, runbooks, permissions, escalation paths, and evidence-delivery commitments. A control is not sustainable if success depends on an unwritten assumption between organizations.

Management should also be able to tell whether the process remains effective over time. Useful indicators include coverage of the expected population, completion of required reviews, age of exceptions, repeated failure patterns, evidence retrievability, provider response time, and successful validation tests. The goal is not to create a compliance score for every activity. It is to make deterioration visible early enough to correct it before it becomes an incident, contract issue, or assessment finding.

For governance topics, Harbor Point uses a simple test: could a backup owner explain the current state, identify the authoritative records, and take the next required action without relying on one person’s memory? If not, the process is still person-dependent and should be strengthened before leadership treats it as sustained.

Evidence to Preserve: baseline ownership; current SSP and scope; recurring review calendar; open exceptions

MSP implementation note: Do not create a separate compliance organization that discovers

changes only after operations have already moved on.

16.2 Establish the Continuous-Readiness Operating Model

Establish the Continuous-Readiness Operating Model matters because a governance model that links security work to CMMC-relevant outcomes. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: governance charter; role matrix; meeting cadence; escalation thresholds

MSP implementation note: Make existing operational forums carry readiness actions whenever possible instead of adding meetings that no one uses.

16.3 Assign One Accountable Owner for the Program

Assign One Accountable Owner for the Program matters because clear accountability for the sustained condition of the assessed environment. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: executive owner designation; program RACI; delegated authorities; backup owner

MSP implementation note: The MSP can operate controls, but the customer should know who has authority to make scope, risk, and compliance decisions.

16.4 Maintain a Dated Readiness Baseline

Maintain a Dated Readiness Baseline matters because a controlled snapshot of scope, systems, providers, responsibilities, and evidence sources. In a continuously managed

environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: baseline package; approval date; version history; source inventories

MSP implementation note: A dated baseline gives the organization a reference point for deciding whether later changes are material.

16.5 Build a Recurring Review Calendar

Build a Recurring Review Calendar matters because review cadences that match the rate at which different controls and records can deteriorate. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: annual calendar; monthly/quarterly review tasks; owners; completion records

MSP implementation note: Automate reminders, but require evidence of completion rather than treating a recurring ticket as proof that the review happened.

16.6 Separate Routine Operations from Management Review

Separate Routine Operations from Management Review matters because the difference between daily control performance and periodic oversight of whether the control remains effective. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: operational tickets; management review minutes; exception trends; corrective actions

MSP implementation note: Do not ask the same engineer who performs every task to be the only

person deciding whether the process is healthy.

16.7 Maintain the Responsibility Matrix as an Operating Record

Maintain the Responsibility Matrix as an Operating Record matters because shared responsibility that changes with services, personnel, and providers. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: current CRM; service descriptions; change approvals; provider contacts

MSP implementation note: Review the matrix against actual permissions, tickets, and contracts rather than accepting old responsibility statements at face value.

16.8 Define Readiness Triggers, Not Just Review Dates

Define Readiness Triggers, Not Just Review Dates matters because event-driven triggers that force review when material conditions change. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: trigger register; change categories; escalation workflow; impact decisions

MSP implementation note: Use change tickets, procurement workflows, HR events, and provider notices as automated or procedural triggers.

16.9 Keep the SSP Synchronized with Reality

Keep the SSP Synchronized with Reality matters because ongoing SSP maintenance as architecture and process evolve. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: current SSP; diagrams; system inventory; revision log; approval record

MSP implementation note: Update the SSP when the environment changes rather than treating SSP maintenance as an annual writing exercise.

16.10 Monitor Control Health, Not Just Tool Health

Monitor Control Health, Not Just Tool Health matters because control-health measures that show whether the intended security outcome is actually being achieved. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

For continuous-monitoring topics, the strongest proof is a time series rather than a single current screenshot. Harbor Point preserves recurring outputs and exception history so an evaluator or manager can see whether the control stayed healthy, how failures were detected, and how quickly they were corrected.

Evidence to Preserve: control-health dashboard; coverage metrics; exception records; validation tests

MSP implementation note: A green product dashboard is not enough if the expected asset population or business process is not represented.

16.11 Reconcile Asset Inventory to Security Coverage

Reconcile Asset Inventory to Security Coverage matters because recurring comparison of in-scope assets to EDR, vulnerability, logging, configuration, and

backup coverage. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: asset inventory; tool exports; reconciliation report; exception tickets

MSP implementation note: Use customer-specific reconciliation across tools so missing agents or stale records do not remain invisible.

16.12 Review Identity and Privileged Access Recurringly

Review Identity and Privileged Access Recurringly matters because periodic validation of users, roles, administrative paths, service accounts, and emergency access. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: access review; privileged-role export; service-account inventory; approvals

MSP implementation note: Build reports from authoritative identity sources and ensure MSP administrators are included in customer-specific reviews.

16.13 Measure Logging and Monitoring Coverage

Measure Logging and Monitoring Coverage matters because sustained visibility across required log sources and alert workflows. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: log-source inventory; ingestion-health report; alert test; retention report

MSP implementation note: Test end-to-end event generation periodically instead of assuming

configured connectors are still delivering usable events.

16.14 Maintain Vulnerability and Patch Closure Discipline

Maintain Vulnerability and Patch Closure Discipline matters because continuous finding intake, prioritization, correction, verification, and exception handling. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: scan results; patch records; exception approvals; re-test results

MSP implementation note: Reconcile vulnerability platforms to the in-scope asset population and investigate authentication failures, not just high CVSS scores.

16.15 Monitor Secure Configuration Drift

Monitor Secure Configuration Drift matters because detection and correction of deviation from approved baselines. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: baseline exports; drift alerts; approved exceptions; change tickets

MSP implementation note: Distinguish approved change from unexplained drift so automation does not repeatedly overwrite legitimate decisions.

16.16 Test Backup and Recovery Readiness

Test Backup and Recovery Readiness matters because sustained proof that protected data can be recovered to an approved destination. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of

truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: backup coverage; restore-test plan; test results; failed-job remediation

MSP implementation note: Restoration testing should validate both technical recovery and the security of the recovery destination.

16.17 Maintain Evidence Health

Maintain Evidence Health matters because evidence generation, retention, attribution, and retrieval as recurring control objectives. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: evidence-health report; retrieval test; retention check; custodian map

MSP implementation note: Test whether customer-specific evidence can still be produced after staff turnover, platform migration, or retention changes.

16.18 Track Exceptions as First-Class Records

Track Exceptions as First-Class Records matters because visible management of temporary deviations, compensating actions, expiration, and closure. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: exception register; approvals; expiration dates; compensating actions; closure proof

MSP implementation note: Do not allow “temporary” provider or customer exceptions to become undocumented permanent architecture.

16.19 Integrate CMMC Impact into Change Management

Integrate CMMC Impact into Change Management matters because security and assessment impact review before changes reach production. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

For change topics, the review is most effective before implementation. The team records the pre-change condition, expected security effect, required document or scope updates, validation plan, and rollback decision. After implementation, it verifies the result and closes the record only when the new state is understood and supportable.

Evidence to Preserve: change request impact field; approvals; updated diagrams; validation results

MSP implementation note: Make CMMC impact one part of normal change review, not a late compliance veto.

16.20 Define Material-Change Escalation

Define Material-Change Escalation matters because criteria for elevating major business or technical changes for management and assessment review. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: material-change criteria; decision record; legal/contract review; revised scope package

MSP implementation note: When uncertainty exists, escalate early and preserve the reasoning rather than letting a major change proceed on an assumption.

16.21 Govern Cloud and SaaS Feature Changes

Govern Cloud and SaaS Feature Changes matters because review of new services, integrations, storage locations, support paths, and administrative features. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: cloud change review; data-flow update; shared-responsibility record; provider evidence

MSP implementation note: A previously acceptable service can become a new scope path when a feature or integration changes how information is processed.

16.22 Manage MSP Platform Changes

Manage MSP Platform Changes matters because customer impact when RMM, PSA, identity, documentation, backup, EDR, or SIEM platforms change. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: platform transition plan; customer impact assessment; evidence migration; rollback plan

MSP implementation note: Provider modernization should include customer-specific scope and evidence continuity requirements.

16.23 Control Provider and Subcontractor Transitions

Control Provider and Subcontractor Transitions matters because security, data, credential, evidence, and responsibility continuity during vendor changes. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or

trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: offboarding plan; evidence export; credential revocation; new provider CRM

MSP implementation note: A provider transition is complete only when access, data, evidence, monitoring, and contractual responsibilities have all been reconciled.

16.24 Evaluate New Locations and Remote Work Patterns

Evaluate New Locations and Remote Work Patterns matters because impact of offices, home environments, alternate sites, and travel on physical and technical safeguards. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: site review; remote-work approval; asset/location records; physical controls

MSP implementation note: Do not assume a user moving to a new work pattern leaves the existing scope and protection model unchanged.

16.25 Govern Network and Architecture Changes

Govern Network and Architecture Changes matters because impact of segmentation, VPN, zero-trust gateways, firewall redesign, and connectivity changes. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: network diagram; rule review; change approval; test results

MSP implementation note: Require before-and-after evidence so the team can prove that intended boundaries and routes still work after change.

16.26 Manage Technology End of Life

Manage Technology End of Life matters because security and evidence risks created by unsupported hardware, software, operating systems, and services. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: lifecycle register; replacement plan; exceptions; compensating actions

MSP implementation note: The MSP should surface end-of-life risk early enough for the customer to fund and schedule replacement.

16.27 Incorporate Business Acquisitions and Divestitures

Incorporate Business Acquisitions and Divestitures matters because scope, identity, data, provider, and contractual consequences of organizational change. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: M&A security review; new asset/provider inventory; access cleanup; scope decision

MSP implementation note: Treat mergers and divestitures as architecture events, not merely legal or financial events.

16.28 Review Procurement Before Purchase

Review Procurement Before Purchase matters because security and CMMC review of products and services before they become embedded dependencies. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: procurement checklist; security requirements; provider evidence; approval record

MSP implementation note: The cheapest time to reject an unsuitable service is before purchase, not after CUI workflows depend on it.

16.29 Prepare the Annual Affirmation as a Management Decision

Prepare the Annual Affirmation as a Management Decision matters because annual affirmation supported by current scope, evidence, change review, and unresolved-risk visibility. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

For official records and management oversight, Harbor Point uses reconciliation rather than assumption. The internal environment, contracts, SPRS/CMMC records, provider status, and executive reports should describe the same system and time period. Differences are treated as records-management and governance issues that require correction.

Evidence to Preserve: affirmation package; management review; scope confirmation; signed affirmation record

MSP implementation note: Do not reduce affirmation to a portal task delegated to someone who lacks visibility into material changes.

16.30 Maintain Accurate CMMC UID and SPRS Records

Maintain Accurate CMMC UID and SPRS Records matters because ongoing accuracy of system identifiers, assessment records, and official cyber records. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: CMMC UID map; SPRS screenshots/exports; change log; correction

tickets

MSP implementation note: Assign one accountable business process for reconciling internal system names to official identifiers.

16.31 Confirm Current Status Before Contract Decisions

Confirm Current Status Before Contract Decisions matters because validation of CMMC status, assessment age, conditional closeout, and contract applicability before representations. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: status verification; contract review; decision memo; renewal calendar

MSP implementation note: MSPs should not make customer-facing certification claims based on stale internal spreadsheets.

16.32 Coordinate Contract and Solicitation Changes

Coordinate Contract and Solicitation Changes matters because review of new clauses, modifications, option periods, and changed CMMC level requirements. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: contract review record; requirement matrix; implementation decision; customer notification

MSP implementation note: Security teams need a trigger from contracting personnel when cyber clauses change.

16.33 Sustain Subcontractor Flowdown Governance

Sustain Subcontractor Flowdown Governance matters because ongoing verification that required subcontractor status, affirmation, and safeguarding obligations remain current. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: subcontract inventory; flowdown clauses; status checks; supplier attestations

MSP implementation note: Treat supplier status as a monitored dependency rather than a one-time onboarding document.

16.34 Govern External Service Provider Evidence

Govern External Service Provider Evidence matters because recurring confirmation that provider evidence remains current, applicable, customer-specific, and retrievable. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: provider evidence calendar; service-specific reports; SLA; exceptions

MSP implementation note: Build evidence delivery into the service contract instead of depending on favors during assessment preparation.

16.35 Maintain Executive Readiness Reporting

Maintain Executive Readiness Reporting matters because decision-oriented reporting on scope, control health, exceptions, provider risk, evidence, and upcoming obligations. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: executive dashboard; risk decisions; action log; trend reports

MSP implementation note: Report a small set of meaningful indicators rather than overwhelming leadership with tool-generated counts.

16.36 Use Metrics That Reveal Drift and Recurrence

Use Metrics That Reveal Drift and Recurrence matters because measures that expose deterioration, aging, and repeated root causes. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: metric definitions; trends; thresholds; corrective actions

MSP implementation note: Measure time to detect drift, repeat findings, exception age, coverage gaps, and evidence retrieval—not just ticket closure volume.

16.37 Preserve Independent Validation

Preserve Independent Validation matters because periodic challenge of control assumptions through internal audit, peer review, sampling, or external readiness support. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: validation plan; sample records; findings; corrective actions

MSP implementation note: Use personnel independent of daily execution when practical for high-impact controls and recurring weaknesses.

16.38 Keep a Readiness Risk Register

Keep a Readiness Risk Register matters because consolidated view of unresolved risks, assumptions, provider dependencies, and decisions. In a continuously managed

environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: risk register; owners; due dates; decision records; closure evidence

MSP implementation note: A single risk view helps prevent the same issue from being hidden across security, IT, compliance, and vendor-management systems.

16.39 Harbor Point Case: Identity Drift After a Reorganization

Harbor Point Case: Identity Drift After a Reorganization matters because a reorganization that leaves excessive privileges and outdated group membership. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

The case-study lesson is that continuous readiness is visible in the response to ordinary change. The team identifies the trigger, determines the affected controls and records, assigns the work, validates the outcome, updates the authoritative documentation, and preserves enough evidence to explain the decision later.

Evidence to Preserve: reorganization roster; role review; access changes; validation export

MSP implementation note: Tie HR change events to customer and provider access-review workflows so organization changes trigger technical review.

16.40 Harbor Point Case: The SIEM Connector That Quietly Failed

Harbor Point Case: The SIEM Connector That Quietly Failed matters because monitoring degradation that looks healthy until end-to-end testing reveals missing logs. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats

the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: connector health; generated test event; case record; repair evidence

MSP implementation note: Require source-level heartbeat and test-event validation for critical log paths.

16.41 Harbor Point Case: A New SaaS Integration Changes Scope

Harbor Point Case: A New SaaS Integration Changes Scope matters because a convenient integration that creates a new data path and administrative dependency. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: procurement/change record; data-flow map; provider review; revised scope decision

MSP implementation note: Make integration approval dependent on information-flow and provider-responsibility review.

16.42 Harbor Point Case: Provider Evidence Retention Shrinks

Harbor Point Case: Provider Evidence Retention Shrinks matters because a service change that shortens available historical evidence below the customer’s operational need. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: provider notice; retention decision; export plan; revised SLA

MSP implementation note: Monitor vendor service notices that can affect evidence availability,

not just uptime and price.

16.43 Harbor Point Case: Annual Affirmation Readiness Review

Harbor Point Case: Annual Affirmation Readiness Review matters because a structured management review before the affirming official submits the annual affirmation. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: affirmation checklist; current scope; material-change log; open-risk summary

MSP implementation note: Provide the AO with concise evidence-backed facts, not a generic statement that “IT says everything is fine.”

16.44 Build a Rolling Twelve-Month Readiness Plan

Build a Rolling Twelve-Month Readiness Plan matters because forward planning that connects reviews, evidence cycles, provider renewals, exercises, assessments, and affirmations. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: annual readiness calendar; owners; dependencies; budget items

MSP implementation note: Use the same calendar for operations and compliance milestones so conflicts become visible early.

16.45 Conduct Quarterly Readiness Exercises

Conduct Quarterly Readiness Exercises matters because short scenario-based exercises that test evidence retrieval, responsibility, technical proof, and decision

paths. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: exercise plan; participant list; findings; corrective actions

MSP implementation note: Rotate scenarios across identity, logging, incident response, provider evidence, backup, and change management.

16.46 Prepare for the Next Assessment Before the Window Opens

Prepare for the Next Assessment Before the Window Opens matters because progressive refresh of scope, evidence, interviews, technical tests, and provider commitments. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: next-cycle plan; evidence refresh; participant readiness; provider schedule

MSP implementation note: Avoid assessment-week freezes that mask the normal operating condition; readiness should be demonstrated in ordinary workflows.

16.47 Turn Lessons Learned into Service Design

Turn Lessons Learned into Service Design matters because using findings, incidents, exercises, and assessment feedback to change recurring MSP services. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: lessons-learned register; service changes; updated runbooks; training

MSP implementation note: When a weakness affects multiple customers, improve the service pattern while preserving customer-specific validation.

16.48 Define the Sustainable MSP CMMC Operating Model

Define the Sustainable MSP CMMC Operating Model matters because an integrated model that keeps security, evidence, responsibilities, contracts, and management aligned over time. In a continuously managed environment, the organization does not wait for an assessment request to discover whether the process still works. Harbor Point treats the subject as part of normal security operations and assigns an owner, an expected cadence or trigger, a source of truth, and a defined way to detect failure. This converts a broad compliance expectation into observable work.

Evidence to Preserve: operating model; service catalog; evidence SLA; governance calendar; metrics

MSP implementation note: The mature MSP product is not “CMMC in a box”; it is a controlled service model that customers can understand, verify, and sustain.

Continuous-Readiness Field Guide for MSP-Supported Organizations

Area	Minimum recurring discipline	Useful evidence	Escalate when
Scope	Reconcile systems, locations, people, information flows, providers, and specialized assets	scope register; diagrams; asset inventory; provider list	new data path, new provider, merger, site move, major platform change
Identity	Review users, privileged roles, service accounts, MFA coverage, emergency access	identity exports; access reviews; tickets; exception records	orphan account, excessive privilege, stale admin, MFA gap
Endpoint	Reconcile assets to EDR, configuration, vulnerability, and patch coverage	coverage exports; drift reports; remediation tickets	unmanaged device, stale agent, unsupported OS
Logging	Check source coverage, ingestion health, retention,	source inventory; heartbeat report; test event; retention	critical source stops, retention shrinks, alert path

Area	Minimum recurring discipline	Useful evidence	Escalate when
	alerting, and time synchronization	report	fails
Vulnerability	Run scans, validate authenticated coverage, prioritize, remediate, re-test	scan history; exceptions; patch/change records; closure test	critical exposure, repeated finding, scan blind spot
Backup	Monitor job health and perform controlled restore tests	backup logs; restore results; failed-job remediation	coverage gap, restore failure, unapproved destination
Provider	Review responsibilities, evidence delivery, access, subcontractors, and service changes	CRM; service reports; SLA; access list; provider notices	service tier change, evidence unavailable, new subprocessors
Evidence	Test generation, attribution, retention, custody, and retrieval	evidence-health review; retrieval tests; custodian map	missing history, mixed-customer data, single-person dependency
Contracts	Review clauses, modifications, CMMC level, UIDs, and flowdown	contract matrix; modification review; subcontract records	new clause, changed level, option renewal, new subcontractor
Affirmation	Prepare evidence-backed annual management review	affirmation package; material-change log; open-risk summary	scope uncertainty, unresolved material change, record mismatch

Continuous-Readiness Implementation Checklist

- Appoint an accountable executive owner and operational program owner with backups.
- Maintain a dated baseline of scope, SSP, inventory, diagrams, providers, and responsibilities.
- Define review cadences and event-driven readiness triggers.
- Reconcile the in-scope asset population to EDR, vulnerability, logging, configuration, patch, and backup coverage.
- Review privileged users, service accounts, emergency access, and MSP administrator access on a defined cadence.
- Generate and test benign security events to verify critical logging and alert paths end to end.

- Monitor evidence generation, retention, attribution, retrieval, and custodian continuity.
- Maintain one controlled exception register with owners, expiration, compensating actions, and closure evidence.
- Add CMMC impact review to normal change-management and procurement workflows.
- Review new SaaS integrations, cloud features, and provider subprocessors before use in protected workflows.
- Manage provider transitions with data, credential, evidence, and responsibility continuity.
- Monitor technology lifecycle and escalate end-of-life systems before support ends.
- Review contract modifications and solicitation changes for revised cyber obligations.
- Maintain current subcontractor flowdown records and status verification.
- Reconcile official CMMC UIDs and applicable SPRS records with the systems actually used for contract performance.
- Prepare annual affirmation as a management review supported by current objective evidence.
- Maintain a readiness risk register and trend high-impact exceptions and repeated root causes.
- Conduct periodic independent validation of high-impact controls and recurring weaknesses.
- Run quarterly readiness exercises that test evidence retrieval, technical proof, and provider coordination.
- Maintain a rolling twelve-month calendar for reviews, renewals, provider evidence, exercises, affirmations, and next-cycle preparation.

Operational Workshops

Workshop 1: Build the Readiness Calendar

Create a twelve-month calendar for Harbor Point that includes access reviews, vulnerability scans, restore tests, provider evidence reviews, annual affirmation preparation, contract renewal reviews, tabletop exercises, and quarterly management reviews. Identify the owner and backup for each event.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.

- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 2: Design Event-Driven Triggers

List ten business or technical events that should trigger an unscheduled CMMC impact review. For each event, identify the affected records and the role that must decide whether scope or security requirements changed.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 3: Reconcile Coverage

Take a sample asset inventory and compare it to EDR, vulnerability, logging, patch, and backup consoles. Record mismatches and decide whether each is an inventory defect, deployment gap, unsupported asset, exception, or stale console record.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 4: Test Evidence Health

Choose five recurring controls and identify the authoritative evidence source, expected generation cadence, retention, custodian, customer attribution, and retrieval method. Perform a mock request for evidence from six months earlier.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.

- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 5: Evaluate a Provider Change

Assume NorthStar is replacing its RMM platform. Build an impact review covering privileged access, customer isolation, logging, evidence history, remote-session controls, ticket integrations, credential storage, subcontractors, and transition rollback.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 6: Review a New SaaS Integration

Assume Harbor Point wants to connect an engineering collaboration platform to Microsoft 365. Trace information flow, identity, administrative roles, logs, support access, retention, exports, and provider responsibilities before approving the integration.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 7: Prepare the Annual Affirmation Package

Create the management package the affirming official should review: current status, CMMC UID, scope confirmation, material changes, open exceptions, provider changes, recent control-health indicators, unresolved incidents, and readiness risks.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.

- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 8: Run a Quarterly Readiness Exercise

Generate a benign privileged-access event and require the team to show approval, provisioning, MFA, logging, SOC visibility, ticket evidence, access-review coverage, and offboarding path. Record weak points and corrective owners.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 9: Test a Contract Change Trigger

Assume a contract modification adds a new performance location and a different required CMMC level. Identify contracting, legal, security, MSP, provider, scope, assessment, and SPRS actions required before performance begins.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Workshop 10: Build the Next-Cycle Plan

Create a six-quarter plan leading to the next assessment window. Sequence scope refresh, internal assessment, evidence refresh, provider commitments, remediation, management review, interview preparation, technical demonstrations, and contingency time.

- Define the objective and success criteria.
- Identify customer, MSP, MSSP, provider, and management roles.
- List the evidence that should be produced naturally by the exercise.
- Record gaps as corrective actions with owners and due dates.
- Identify any SSP, scope, CRM, contract, runbook, or evidence-index updates triggered by the result.

Review Questions

1. Why is continuous readiness different from saying that the environment never changes?
2. What is the value of a dated readiness baseline?
3. Why should recurring review dates be supplemented with event-driven triggers?
4. How does the Customer Responsibility Matrix support sustainment?
5. What makes an SSP a living operating record rather than an assessment document?
6. Why can a green security console still conceal a control failure?
7. What should be reconciled to the authoritative asset inventory?
8. Why should privileged-access reviews include MSP and provider administrators?
9. How can an organization test the logging pipeline end to end?
10. What is the difference between vulnerability discovery and validated closure?
11. Why should secure-configuration drift be distinguished from approved change?
12. What does a successful restore test prove that a successful backup job does not?
13. What characteristics define healthy recurring evidence?
14. Why do temporary exceptions require expiration and closure evidence?
15. At what point should CMMC impact analysis occur in change management?
16. What kinds of changes may justify material-change escalation?
17. How can a new SaaS feature alter scope or responsibility?
18. Why can an MSP platform migration create evidence risk?
19. What should provider offboarding preserve besides data?
20. How can remote work change both technical and physical safeguards?
21. What evidence should accompany a major network redesign?
22. Why is technology end of life a readiness issue?
23. How should mergers or divestitures trigger cybersecurity review?
24. Why should security review occur before procurement?
25. What should the affirming official review before annual affirmation?
26. Why must CMMC UID and SPRS records be reconciled with internal system records?
27. What should be verified before making a contract-status representation?
28. How can a contract modification create new cybersecurity work?

29. Why is subcontractor status a monitored dependency rather than a one-time check?
30. What makes provider evidence dependable over time?
31. Which indicators belong on an executive readiness dashboard?
32. Why is ticket closure count a weak sustainment metric?
33. What value does independent validation add?
34. Why should readiness risks be consolidated across teams?
35. What root cause allowed Harbor Point's identity drift after reorganization?
36. How did the SIEM connector case demonstrate the value of test events?
37. Why did the new SaaS integration require a scope review?
38. What should Harbor Point do when provider retention changes?
39. How should a rolling twelve-month plan reduce assessment risk?
40. What distinguishes a sustainable MSP CMMC operating model from "CMMC in a box"?

Answer Guidance

Questions 1–8 focus on governance, baselines, scope, responsibilities, SSP maintenance, and population reconciliation. Sustainable readiness requires clear ownership and authoritative records that remain aligned with actual operations.

Questions 9–16 focus on control health, logging, vulnerabilities, configuration, recovery, evidence, exceptions, and change management. The organization should detect degradation through observable tests and manage change before it becomes unexplained drift.

Questions 17–24 focus on cloud, providers, network changes, remote work, lifecycle, organizational change, and procurement. These events can alter information flow, administrative access, evidence, and assessment scope even when the business sees them as ordinary modernization.

Questions 25–32 focus on affirmation, SPRS/CMMC records, contracts, subcontractors, provider evidence, executive reporting, and metrics. Official records and management decisions should be based on current, reconciled facts rather than stale assumptions.

Questions 33–40 focus on independent validation, risk consolidation, case studies, rolling planning, and the mature MSP operating model. Readiness improves when

lessons learned change recurring service design and when the next assessment cycle is prepared through ordinary operations rather than a last-minute project.

Key Terms

Term	Working meaning in this chapter
Continuous Readiness	The sustained ability to demonstrate that the current environment, controls, responsibilities, evidence, and official records remain aligned.
Readiness Baseline	A dated, approved snapshot of scope, systems, providers, responsibilities, evidence sources, and significant assumptions.
Control Health	Observable indicators showing whether a security requirement continues to operate as intended across its expected population.
Drift	Unapproved or unexplained deviation between the approved state and the current technical or operational state.
Material Change	A business, technical, provider, location, information-flow, or organizational change significant enough to require elevated review of scope, controls, or status.
Evidence Health	The continued ability to generate, retain, attribute, retrieve, and explain objective records of control operation.
Readiness Trigger	A scheduled or event-driven condition that requires security, scope, responsibility, or evidence review.
Exception	A documented, approved deviation with defined scope, risk treatment, owner, duration, and closure criteria.
Annual Affirmation	The recurring management affirmation of continuous compliance required by applicable CMMC rules and contract clauses.
CMMC UID	The unique identifier associated with the contractor information system/CMMC record used in the applicable SPRS process.
Provider Evidence SLA	A service commitment defining what customer-specific security evidence a provider will produce, how often, how quickly, and in what form.
Readiness Risk Register	A consolidated record of unresolved security, scope,

Term	Working meaning in this chapter
	provider, evidence, contractual, or governance risks affecting sustained readiness.

Practical Templates

Continuous-Readiness Review Record

Review period	_____
Baseline/version reviewed	_____
Scope changes identified	_____
Control-health exceptions	_____
Provider changes	_____
Evidence-health issues	_____
Contract/subcontract changes	_____
Open corrective actions	_____
Management decisions	_____
Next review date	_____

Material-Change Decision Record

Change description	_____
Business owner	_____
Systems/providers affected	_____

	_
Information-flow change	_____ _
Administrative-access change	_____ _
Security-control impact	_____ _
Scope/SSP impact	_____ _
Evidence impact	_____ _
Contract/affirmation impact	_____ _
Decision and approver	_____ _

Evidence Health Review

Evidence source	_____ _
Control/requirement supported	_____ _
Expected cadence	_____ _
Last successful generation	_____ _
Retention available	_____ _
Customer attribution verified	_____ _
Retrieval test result	_____ _
Custodian and backup	_____ _
Known limitations	_____ _

Corrective owner	_____ _

Annual Affirmation Preparation Record

CMMC UID	_____ _
Current status/date	_____ _
Scope confirmed	_____ _
Material changes reviewed	_____ _
Open exceptions	_____ _
Provider changes reviewed	_____ _
Control-health summary	_____ _
Evidence-health summary	_____ _
Contract changes reviewed	_____ _
AO decision/affirmation date	_____ _

Provider Sustainment Review

Provider/service	_____ _
Customer responsibilities	_____ _
Provider responsibilities	_____ _
Administrative access	_____ _

Subprocessors	_____
Evidence deliverables	_____
Retention	_____
Recent service changes	_____
Open incidents/exceptions	_____
Renewal or corrective decision	_____

Chapter Closing

CMMC readiness is easiest to lose in ordinary operations. The assessment ends, the remediation project closes, and attention moves to new business priorities. Then a new administrator is added, a cloud integration appears, an MSP changes platforms, a log connector fails, an exception expires without review, or a contract modification changes the requirement. None of these events looks dramatic by itself. Together they can make the assessed environment materially different from the one management believes it still operates.

The sustainable answer is not permanent change freeze. It is disciplined change. Harbor Point keeps a current baseline, uses triggers and recurring reviews, measures control health, reconciles evidence and population coverage, manages provider dependencies, and escalates material change. NorthStar embeds these practices into service delivery instead of running a separate compliance workflow. Beacon validates that monitoring and incident capabilities remain alive. Management receives concise facts that support decisions and annual affirmation.

The mature operating model therefore makes readiness a by-product of good security management. The same records used to administer users, change systems, investigate alerts, patch vulnerabilities, test backups, review providers, and approve risk also preserve the evidence needed to explain the environment later. Assessment preparation becomes an organized retrieval and validation exercise rather than an attempt to reconstruct a year of operations.

That is the standard for the remaining chapters of this book: not merely achieving a status, but building services and governance that can sustain trustworthy cybersecurity over the full contract and assessment lifecycle.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Consult the current edition for assessment, affirmation, status, POA&M, scoping, and external-service-provider requirements.

R2. Acquisition.gov. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025). Includes requirements to maintain the specified CMMC status for the duration of the contract, complete annual affirmations in SPRS, maintain applicable CMMC UIDs, and flow down requirements as required.

R3. Department CMMC resources and July 13, 2026 announcement suspending Phase II requirements while maintaining Phase I self-assessment requirements and continuing the program review. Confirm current implementation status before relying on future transition dates.

R4. National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, as used by the published CMMC Level 2 framework discussed in this book.

R5. National Institute of Standards and Technology. NIST SP 800-171A (June 2018), assessment procedures associated with the Revision 2 baseline referenced by the CMMC Level 2 assessment framework discussed in this book.

R6. Acquisition.gov. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, for applicable safeguarding, cloud-service, incident-reporting, preservation, and flowdown requirements.

R7. Acquisition.gov. DFARS 252.204-7019 and 252.204-7020, for applicable NIST SP 800-171 DoD Assessment and SPRS requirements distinct from CMMC assessment records.

R8. Current Department CMMC Resources & Documentation page, FAQs, official implementation memoranda, and SPRS guidance. Organizations should verify current procedures whenever submitting or affirming an official record.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance. It does not replace governing regulations, contract clauses, official Department guidance, legal advice, or an authorized CMMC assessment determination.

CMMC for MSPs

From Readiness to Certification

Chapter 17

Working with a C3PAO

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Focus

How an MSP-supported organization selects, contracts with, prepares for, and works with an independent C3PAO while preserving customer accountability, assessor independence, evidence integrity, and a defensible assessment record.

Chapter Contents

- Purpose, learning objectives, current source context, and operating principles
- 17.1–17.8 Understanding the C3PAO relationship and preparing to engage
- 17.9–17.16 Selecting, contracting with, and onboarding a C3PAO
- 17.17–17.24 Scope alignment, pre-assessment coordination, evidence exchange, and logistics
- 17.25–17.34 Assessment execution: examine, interview, test, daily management, and provider participation
- 17.35–17.42 Findings, factual corrections, conditional status, POA&M closeout, appeals, and certification records
- 17.43–17.48 Harbor Point case study, lessons learned, and post-assessment sustainment
- C3PAO field guide, implementation checklist, 10 workshops, working templates, 40 review questions, key terms, and official references

Chapter Purpose

Chapter 16 established the operating discipline required to keep a CMMC environment ready after remediation and assessment preparation. Chapter 17 brings that discipline into the external-assessment relationship. The focus is not simply on "passing an assessment." It is on working with an independent CMMC Third-Party Assessment Organization, or C3PAO, in a way that is organized, factual, secure, efficient, and consistent with the real operating environment.

For an MSP-supported contractor, that relationship can become complicated quickly. Harbor Point Engineering owns the contractor information system and the representations made about its CMMC status. NorthStar Managed Technology performs many technical functions and holds important operational records. Beacon Security Operations performs monitoring and incident-response functions. A C3PAO, however, is not another service provider in this chain. It is an independent assessment organization. The C3PAO must be able to evaluate Harbor Point without being directed by NorthStar, coached by the customer, or placed in a commercial relationship that compromises impartiality.

This chapter therefore treats the C3PAO engagement as a governed lifecycle. It begins before procurement, when the organization determines whether a C3PAO assessment is the required pathway and whether the planned assessment scope is stable enough to support an engagement. It continues through selection, contracting, pre-assessment coordination, evidence transfer, interviews, technical demonstrations, findings, factual corrections, conditional status and POA&M closeout when permitted, appeals or complaints, certificate issuance, record retention, and lessons learned.

The goal is to make the real environment understandable. The customer should not stage a performance for assessment week. The MSP should not become the customer's spokesperson. The assessor should not be asked to design the controls it will later evaluate. A strong engagement preserves these boundaries while making evidence, people, systems, and responsibilities available in an orderly way.

Learning Objectives

- Explain the role of a C3PAO and distinguish it from an MSP, MSSP, consultant, Registered Provider Organization, cloud provider, and government assessment organization.
- Determine when a Level 2 C3PAO assessment pathway applies and how the current September 2026 implementation pause affects scheduling assumptions.

- Evaluate prospective C3PAOs for authorization status, independence, conflicts of interest, assessment capability, secure evidence handling, staffing, schedule, and commercial terms.
- Build an assessment contract and statement of work that defines scope assumptions, roles, evidence exchange, logistics, security, communications, fees, change control, and closeout without prescribing assessor conclusions.
- Prepare the customer, MSP, MSSP, cloud providers, and other external service providers for assessment participation while preserving customer accountability.
- Coordinate examine, interview, and test activities without scripting participants or attempting to influence assessment determinations.
- Manage evidence requests, assessor questions, technical demonstrations, remote access, and multi-tenant provider records securely and traceably.
- Distinguish factual corrections from disputes over assessment judgment and understand escalation, appeal, and complaint pathways.
- Manage Conditional status and authorized POA&M closeout when applicable, without treating planned work as implemented security.
- Preserve assessment records, remove temporary access, capture lessons learned, and return the organization to continuous readiness after the engagement.

Source Context and Current Implementation Note

This chapter uses the CMMC Program rule in 32 CFR Part 170, current DFARS implementation language, current Department CMMC resources, the Level 2 assessment guidance, and current Cyber AB ecosystem requirements as its principal sources. The formal source should always control over a training slide, consultant checklist, or provider interpretation.

Current implementation timing matters. On July 13, 2026, the Department announced the immediate suspension of CMMC Phase II requirements that had been scheduled for November 10, 2026. Phase I self-assessment requirements remain in place while the Department conducts a broader review. This does not erase the C3PAO assessment framework or make the operational disciplines in this chapter irrelevant. It does mean that an organization should verify the current solicitation, contract, and Department implementation notices before assuming that a previously announced C3PAO timeline still applies.

The current DFARS 252.204-7021 clause defines contractor obligations when CMMC is required by a contract, including maintaining current CMMC status for the duration of the contract, annual affirmation in SPRS for each applicable CMMC UID, and successful closeout of a valid POA&M when the contractor holds Conditional status. The organization should therefore connect assessment planning to contract

review rather than treating certification scheduling as a stand-alone compliance project.

17.1 Understand What a C3PAO Is - and Is Not

A C3PAO is an independent organization authorized within the CMMC ecosystem to conduct applicable Level 2 certification assessments. It is not the customer’s managed service provider, compliance consultant, virtual CISO, or technical implementer.

Engagement governance requires Harbor Point to define the C3PAO's independent assessment role before assigning work. The accountable participants are the executive sponsor, assessment coordinator, procurement lead, and provider liaisons. They should work from a role-and-authority statement tied to the engagement charter, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is treating the assessor as a consultant or treating the MSP as the assessed organization. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

The operating test is practical: another qualified person should be able to reconstruct the decision and repeat the process from the retained record. The record should identify the applicable system and time period, the customer and provider responsibilities, the source data reviewed, exceptions or limitations, the approval authority, and the next required action. A screenshot or meeting note may support that record, but neither substitutes for attribution, scope, and approval.

Recommended operating sequence:

- 1. Name the organization seeking assessment.
- 2. Identify the systems and locations.
- 3. Distinguish customer, provider, consultant, and assessor duties.
- 4. Approve one escalation path.

Before closing this activity, the assessment coordinator should challenge the result from the assessor's perspective: Is the source authoritative? Does it apply to Harbor Point's assessed system? Does it cover the relevant period? Can the responsible person explain it without relying on a script? Is any customer, provider, or tenant information missing or overexposed? Negative answers should create tracked actions with owners and dates, not undocumented verbal assurances.

Evidence to Preserve: C3PAO authorization record; independence review; engagement decision memo

MSP implementation note: Do not market the C3PAO as part of the MSP's delivery team. Independence should remain visible in contracts, communications, and meeting roles.

17.2 Start with the Contractual Assessment Path

Before contacting a C3PAO, the organization should determine the CMMC level and assessment type tied to the actual solicitation, contract, or business objective. A readiness goal should not be mistaken for a contractual assessment mandate.

Engagement governance requires Harbor Point to trace the assessment pathway to the solicitation, contract, or documented business decision. The accountable participants are contracts, legal counsel, the affirming official, and the CMMC program owner. They should work from a dated requirement determination with the controlling clause and system applicability, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is buying an assessment that does not match the contractual requirement or missing one that does. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Read the controlling instrument.

- 2. Identify the required level and assessment type.
- 3. Map it to each contractor information system.
- 4. Obtain management approval.

Evidence to Preserve: contract clauses; solicitation language; CMMC level determination; legal/procurement review

MSP implementation note: The MSP can summarize technical implications but should not decide the customer's contractual requirement.

17.3 Confirm Current Program Timing Before Scheduling

Implementation schedules can change. Harbor Point therefore checks current Department notices before locking a certification date or telling a customer that a C3PAO assessment is immediately required.

Engagement governance requires Harbor Point to base scheduling on current official implementation information. The accountable participants are the program owner, contracts lead, procurement lead, and executive sponsor. They should work from a dated scheduling memorandum with source links and assumptions, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is building budget, customer promises, or staffing plans around an obsolete rollout date. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Check current Department notices.
- 2. Compare them with each live procurement.
- 3. Separate regulatory timing from voluntary readiness goals.
- 4. Set a review trigger for new guidance.

Evidence to Preserve: current DoD notice; schedule decision; procurement assumptions

MSP implementation note: Use dated official sources and preserve the source relied upon for the scheduling decision.

17.4 Stabilize Scope Before Commercial Engagement

A C3PAO estimate depends heavily on the system boundary, sites, users, technologies, external providers, and assessment complexity. Major unresolved scope questions create rework and commercial disputes.

Engagement governance requires Harbor Point to present a sufficiently stable assessment boundary for estimating and planning. The accountable participants are the system owner, security architect, asset owner, facilities lead, and provider technical leads. They should work from a versioned scope package containing diagrams, inventories, locations, data flows, and provider dependencies, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is discovering material enclaves, remote users, cloud services, or external connections after the price and schedule are fixed. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Reconcile the SSP and diagrams.
- 2. Classify assets.
- 3. Validate locations and remote work.
- 4. Confirm provider and subcontractor dependencies.
- 5. Record unresolved assumptions.

Evidence to Preserve: scope diagram; asset categories; locations; provider inventory; SSP baseline

MSP implementation note: Do not ask the C3PAO to discover the entire scope for the first time after the assessment contract is signed.

17.5 Know the Difference Between Readiness and Assessment

Internal readiness reviews may identify gaps and prepare evidence. The formal assessment determines conformity. The organizations performing these activities should be described accurately.

Engagement governance requires Harbor Point to keep remediation advice separate from formal assessment judgment. The accountable participants are the readiness lead, legal counsel, procurement, and the proposed C3PAO. They should work from a service map that labels readiness, consulting, assessment, and remediation activities, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is allowing the formal assessment team to design the implementation it will later judge. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Inventory prior advisory work.
- 2. Identify organizational and personnel overlaps.
- 3. Obtain conflict disclosures.
- 4. Assign remediation to an independent party.
- 5. Preserve the boundary in communications.

Evidence to Preserve: readiness report; engagement labels; assessor role statement

MSP implementation note: Never call an MSP readiness review a certification assessment.

17.6 Preserve Assessor Independence

The C3PAO must be free to make assessment determinations based on evidence and applicable requirements. Customer pressure, contingent fees tied to outcomes, or

assessment-team involvement in designing the evaluated implementation can create unacceptable conflicts.

Engagement governance requires Harbor Point to protect the impartiality of assessment decisions. The accountable participants are procurement, legal counsel, the executive sponsor, and the C3PAO's designated independence contact. They should work from a conflict-of-interest review and written resolution of disclosed relationships, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is using referral, consulting, payment, or schedule pressure to influence conclusions. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Collect disclosures.
- 2. Examine ownership and referral relationships.
- 3. Review prior services.
- 4. Remove outcome-contingent incentives.
- 5. Document the final independence determination.

Evidence to Preserve: conflict-of-interest review; procurement records; independence attestations

MSP implementation note: Keep remediation consulting and formal assessment roles clearly separated.

17.7 Build an Internal Assessment Governance Team

Harbor Point designates an executive sponsor, assessment coordinator, technical lead, evidence coordinator, legal/contract contact, facilities contact, and provider liaisons. The team has clear authority and backups.

Engagement governance requires Harbor Point to give one customer team authority to coordinate the engagement. The accountable participants are an executive sponsor, assessment coordinator, evidence lead, technical lead, contracts contact, facilities contact, and provider liaisons. They should work from a governance roster with decision rights, backups, contact methods, and availability, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is letting requests bounce among the customer and providers without an accountable decision maker. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Assign primary and backup roles.
- 2. Define who may release evidence.
- 3. Define who may accept schedule changes.
- 4. Publish escalation thresholds.
- 5. Test the roster before kickoff.

Evidence to Preserve: governance roster; RACI; escalation tree; backup assignments

MSP implementation note: The MSP liaison should coordinate provider resources without replacing the customer assessment coordinator.

17.8 Define Success Correctly

Success means an accurate, efficient, secure assessment that reflects the real environment. It does not mean hiding findings, steering assessors, or optimizing appearances.

Engagement governance requires Harbor Point to define success as a fair and supportable assessment of the real environment. The accountable participants are the executive sponsor, affirming official, program owner, and assessment coordinator.

They should work from approved success criteria covering safety, accuracy, evidence integrity, and timely issue handling, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Before procurement advances, management should require a decision that can be explained later. The record must show not only what was decided, but which facts and authorities supported it.

The principal failure mode is equating success only with a desired score and encouraging concealment or unsafe demonstrations. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. State non-negotiable integrity rules.
- 2. Define operational and recordkeeping goals.
- 3. Set stop-work authority for unsafe activity.
- 4. Explain how findings will be handled.

Evidence to Preserve: assessment charter; executive expectations; ethics note

MSP implementation note: Set expectations with leadership before assessment pressure begins.

17.9 Verify C3PAO Authorization and Standing

The organization should confirm that the selected C3PAO is currently authorized for the work it will perform and verify relevant status through current ecosystem sources.

Selection and contracting requires Harbor Point to confirm that the chosen organization is currently eligible to perform the intended work. The accountable participants are procurement, legal counsel, and the assessment coordinator. They should work from a dated verification record showing the listing checked, status observed, legal entity, and scope of authorization, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is relying on a logo, old proposal, affiliate name, or salesperson's statement. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Check the authoritative ecosystem listing.
- 2. Match the legal entity to the contract.
- 3. Confirm the intended assessment service.
- 4. Repeat the check before kickoff and material substitutions.

Evidence to Preserve: authorization verification; date checked; procurement record

MSP implementation note: Re-check status before the formal assessment begins if the procurement cycle is long.

17.10 Evaluate Experience Against Your Actual Environment

Harbor Point evaluates whether the C3PAO has experience with the technologies, architecture patterns, locations, cloud services, specialized assets, and provider-heavy environments in the planned scope.

Selection and contracting requires Harbor Point to select a team that understands the technologies and operating model actually in scope. The accountable participants are the technical lead, security architect, provider liaisons, and procurement. They should work from a capability matrix mapped to the enclave, cloud services, MSP platforms, locations, and specialized assets, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is choosing on generic credentials while the team lacks experience with the environment's material dependencies. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who

may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Describe the architecture without oversharing sensitive data.
- 2. Ask for comparable experience.
- 3. Assess provider and multi-tenant familiarity.
- 4. Identify specialist needs.
- 5. Score responses consistently.

Evidence to Preserve: capability questionnaire; reference checks; technical-fit notes

MSP implementation note: Fit is more important than brand familiarity alone.

17.11 Evaluate Secure Evidence-Handling Practices

The C3PAO may receive sensitive diagrams, configurations, logs, policies, system inventories, and security protection data. The engagement should define secure transfer, access, storage, retention, return, and destruction practices.

Selection and contracting requires Harbor Point to ensure assessment evidence is protected throughout its lifecycle. The accountable participants are the security officer, privacy or legal counsel, evidence lead, and C3PAO security contact. They should work from an evidence-handling plan covering transfer, access, storage, incident notice, retention, return, and destruction, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is moving sensitive configurations, logs, or CUI through unapproved channels or retaining copies indefinitely. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Classify likely artifacts.
- 2. Approve transfer mechanisms.
- 3. Enforce named access.
- 4. Define breach notification.
- 5. Set retention and destruction terms.
- 6. Verify closure.

Evidence to Preserve: evidence-handling terms; encryption method; access controls; retention terms

MSP implementation note: Avoid ordinary email attachments for sensitive assessment evidence unless specifically approved and protected.

17.12 Evaluate Assessment Staffing and Continuity

Ask who will lead the assessment, which roles may participate, how substitutions are handled, and how continuity is maintained if a team member becomes unavailable.

Selection and contracting requires Harbor Point to lock down team composition and manage substitutions deliberately. The accountable participants are the assessment coordinator, procurement, and C3PAO engagement lead. They should work from a staffing schedule listing roles, qualifications, availability, locations, and substitution rules, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is losing context or specialist coverage when personnel change during the engagement. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Review proposed roles.
- 2. Identify key-person dependencies.
- 3. Confirm interview and travel availability.

- 4. Require notice of substitutions.
- 5. Repeat independence and access checks for replacements.

Evidence to Preserve: staffing plan; role qualifications; substitution process

MSP implementation note: Provider staff should know whom to contact but should not bypass the Lead Assessor.

17.13 Understand Pricing Drivers

Assessment fees may reflect scope size, complexity, locations, evidence quality, travel, technical testing, scheduling, and closeout work. Harbor Point compares assumptions rather than comparing only total price.

Selection and contracting requires Harbor Point to compare commercial proposals using the assumptions that create cost. The accountable participants are procurement, the assessment coordinator, technical lead, and finance. They should work from a normalized pricing worksheet for scope, sites, team days, travel, evidence review, retesting, and change requests, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is selecting the lowest total without recognizing exclusions or unrealistic scope assumptions. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Issue the same baseline to bidders.
- 2. Require assumptions and exclusions.
- 3. Compare labor and travel models.
- 4. Price likely changes.
- 5. Document the best-value decision.

Evidence to Preserve: pricing assumptions; scope basis; travel terms; change-order terms

MSP implementation note: Low pricing based on unrealistic scope assumptions can become expensive later.

17.14 Avoid Outcome-Based Commercial Terms

Commercial terms should not reward a favorable determination or create pressure on assessor judgment. Payment should be based on defined services, not the desired certification outcome.

Selection and contracting requires Harbor Point to keep compensation independent of the assessment result. The accountable participants are procurement, legal counsel, finance, and the executive sponsor. They should work from approved fee terms based on work performed rather than certification outcome, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is creating real or perceived pressure through success fees, refunds tied to findings, or referral arrangements. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Remove pass guarantees.
- 2. Prohibit outcome bonuses.
- 3. Disclose referral economics.
- 4. Price optional work separately.
- 5. Document legal and independence review.

Evidence to Preserve: fee schedule; legal review; conflict review

MSP implementation note: Never offer a bonus for “passing.”

17.15 Use a Clear Statement of Work

The SOW should identify the assessment type, organization, expected scope, locations, anticipated timing, coordination expectations, deliverables, evidence transfer approach, security requirements, commercial assumptions, and change control.

Selection and contracting requires Harbor Point to translate the engagement into an executable statement of work. The accountable participants are procurement, legal counsel, the assessment coordinator, security, and the C3PAO. They should work from a signed SOW with scope assumptions, locations, schedule, roles, deliverables, security terms, communications, and closeout, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is leaving critical logistics to informal email and discovering incompatible expectations during assessment week. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Define the baseline.
- 2. State responsibilities.
- 3. Establish evidence and access rules.
- 4. Describe deliverables and acceptance.
- 5. Attach change control.
- 6. Resolve inconsistencies before signature.

Evidence to Preserve: signed SOW; scope attachment; schedule; contacts

MSP implementation note: Keep the SOW operationally specific but do not tell the assessor what conclusion to reach.

17.16 Define Change Control Before Work Starts

If the scope, locations, dates, provider participation, or technology changes materially, the parties need a controlled method to evaluate effect on schedule, effort, and evidence.

Selection and contracting requires Harbor Point to control changes to scope, schedule, staffing, locations, and effort. The accountable participants are the assessment coordinator, procurement, technical lead, and C3PAO engagement lead. They should work from a change log with request, impact, authorization, cost, schedule, and baseline version, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Commercial diligence is part of assessment integrity. A well-written proposal is not enough; the organization must test the assumptions, people, security practices, and boundaries behind it.

The principal failure mode is allowing small verbal changes to accumulate into an unplanned or disputed engagement. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Define change thresholds.
- 2. Require written impact analysis.
- 3. Identify approval authority.
- 4. Update affected plans.
- 5. Communicate the approved baseline to participants.

Evidence to Preserve: change-control procedure; change log; approvals

MSP implementation note: Escalate scope changes immediately instead of hoping they remain unnoticed.

17.17 Conduct a Formal Kickoff

The kickoff aligns roles, communication channels, scope assumptions, evidence-transfer methods, schedules, facilities, remote access, and open questions.

Pre-assessment coordination requires Harbor Point to turn the contract into a shared operating plan. The accountable participants are the executive sponsor, assessment coordinator, evidence lead, technical lead, provider liaisons, and C3PAO team. They should work from kickoff minutes with decisions, open issues, contacts, schedule, and action owners, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is using the kickoff as a ceremonial introduction while material assumptions remain unresolved. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Confirm objectives and independence.
- 2. Walk the scope.
- 3. Review evidence and communication channels.
- 4. Validate interviews and tests.
- 5. Close every open item with an owner and date.

Evidence to Preserve: kickoff agenda; attendee list; decisions; action log

MSP implementation note: NorthStar attends as a provider liaison, not as the assessed organization.

17.18 Reconcile the Assessment Scope with the C3PAO

Harbor Point walks through the SSP, diagrams, asset categories, locations, external providers, cloud services, specialized assets, and security protection assets so both sides understand what environment is being presented.

Pre-assessment coordination requires Harbor Point to reach a documented common understanding of what will be assessed. The accountable participants are the system owner, security architect, assessment coordinator, provider leads, and C3PAO. They should work from a reconciled scope record cross-referenced to the SSP, diagrams, asset categories, locations, and service dependencies, because the C3PAO must be

able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is allowing the written SSP, technical reality, and assessor planning model to describe different environments. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Walk the data flow.
- 2. Identify in-scope, security-protection, specialized, and out-of-scope assets.
- 3. Validate locations.
- 4. Map services.
- 5. Record assessor questions and customer resolutions.

Evidence to Preserve: scope reconciliation record; updated diagrams; open-scope issues

MSP implementation note: Do not silently remove difficult assets from the discussion.

17.19 Resolve Material Scope Questions Before the Assessment Window

Open questions about whether a site, service, or provider is part of the environment can consume assessment time and create contradictory evidence. Resolve them as early as possible.

Pre-assessment coordination requires Harbor Point to close material scope questions before the formal assessment window. The accountable participants are the assessment coordinator, contracts lead, system owner, provider owners, and executive sponsor. They should work from a scope-issue register showing decision, authority, impact, and closure evidence, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is forcing a rushed scope decision after interviews or testing has begun. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Triage open questions.
- 2. Obtain provider facts.
- 3. Seek contractual or legal interpretation when needed.
- 4. Update baselines.
- 5. Reprice or reschedule if the impact is material.

Evidence to Preserve: scope issue log; decisions; authoritative source references

MSP implementation note: Treat unresolved provider scope as a risk, not an administrative detail.

17.20 Build the Evidence Exchange Plan

Define what evidence will be staged, what will be produced on request, who can approve release, where artifacts will be transferred, and how customer/provider attribution will be preserved.

Pre-assessment coordination requires Harbor Point to move every artifact through a controlled and traceable exchange process. The accountable participants are the evidence lead, security officer, technical owners, and C3PAO evidence contact. They should work from an evidence exchange plan and request tracker with unique IDs, versions, owners, release approvals, and disposition, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is sending duplicate, stale, mislabeled, overbroad, or unapproved evidence through scattered channels. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may

communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Define intake fields.
- 2. Approve repositories.
- 3. Label tenant, system, date, and objective.
- 4. Review before release.
- 5. Log superseded versions.
- 6. Reconcile disposition at closeout.

Evidence to Preserve: evidence exchange plan; repository permissions; custodian list

MSP implementation note: Separate source repositories from assessment copies and maintain traceability.

17.21 Protect Multi-Tenant Provider Evidence

NorthStar and Beacon may hold records for many customers. They should provide customer-specific views, redacted exports, controlled demonstrations, or other methods that answer the assessment question without exposing unrelated tenants.

Pre-assessment coordination requires Harbor Point to prove customer-specific operation without exposing unrelated tenants. The accountable participants are the MSP security officer, platform owner, customer evidence lead, and C3PAO. They should work from a tenant-safe evidence method for each multi-tenant tool, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is revealing another customer's data, credentials, alert content, or configuration while trying to support the assessed customer. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Prefer tenant-filtered exports.
- 2. Use controlled live views when exports are unsafe.
- 3. Redact and peer-review screenshots.
- 4. Explain platform-wide controls separately.
- 5. Log every disclosure.

Evidence to Preserve: redaction procedure; tenant filter evidence; demonstration plan

MSP implementation note: Never give assessors unrestricted access to a multi-tenant MSP console merely for convenience.

17.22 Plan Interviews Around Real Control Owners

Interviewees should be the people who actually perform, approve, manage, or oversee the process. Job title alone is not enough.

Pre-assessment coordination requires Harbor Point to put the people who perform and own the work in front of assessors. The accountable participants are the assessment coordinator, control owners, supervisors, and provider liaisons. They should work from an interview matrix mapping objectives to primary participants, backups, and supporting records, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is using executives or consultants to recite processes they do not operate. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Map objectives to real roles.
- 2. Confirm availability.
- 3. Review actual procedures.
- 4. Practice locating records.

- 5. Instruct participants to answer honestly and escalate unknowns.

Evidence to Preserve: interview roster; control-owner mapping; backups

MSP implementation note: Prepare people to understand their real process, not to memorize scripted answers.

17.23 Plan Technical Demonstrations Safely

Technical tests should answer defined questions while protecting production availability, secrets, customer data, and unrelated systems. Use safe test objects when appropriate.

Pre-assessment coordination requires Harbor Point to demonstrate mechanisms without creating production risk. The accountable participants are the technical lead, system owner, change manager, provider operator, and C3PAO test lead. They should work from an approved demonstration plan with test object, expected result, safeguards, evidence, and rollback, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is changing live accounts, policies, logging, or network controls without authorization or recovery planning. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Select a safe test object.
- 2. Obtain change approval.
- 3. Protect secrets and unrelated data.
- 4. Define success and stop conditions.
- 5. Capture evidence.
- 6. Restore and verify state.

Evidence to Preserve: demo plan; test accounts; rollback plan; approvals

MSP implementation note: Do not create dangerous production changes just to demonstrate a control.

17.24 Freeze Only What Must Be Stable

An unnecessary organization-wide change freeze can disrupt business; no freeze at all can make evidence inconsistent. Harbor Point identifies which high-risk changes need coordination during the assessment window.

Pre-assessment coordination requires Harbor Point to maintain stability without stopping necessary security and business operations. The accountable participants are change management, the system owner, security operations, the assessment coordinator, and C3PAO. They should work from an assessment-period change plan identifying restricted, allowed, emergency, and notification categories, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The objective is to remove avoidable ambiguity before the assessment clock is running. Open issues should be visible, owned, and resolved through controlled updates to the baseline.

The principal failure mode is creating a broad freeze that delays patches and incident response or conceals the fact that the environment normally changes. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Identify high-risk changes.
- 2. Preserve emergency authority.
- 3. Notify the assessment team of material changes.
- 4. Update evidence.
- 5. Record the post-change baseline.

Evidence to Preserve: change calendar; freeze criteria; emergency-change process

MSP implementation note: Continue normal security operations; coordinate material changes rather than hiding them.

17.25 Manage the Opening Assessment Session

The opening session confirms participants, scope, schedule, communication paths, evidence handling, safety rules, and daily operating rhythm.

Assessment execution requires Harbor Point to establish the rules of engagement at the opening session. The accountable participants are the executive sponsor, assessment coordinator, C3PAO lead, evidence lead, and provider liaisons. They should work from opening-session minutes confirming scope, schedule, communications, safety, evidence handling, and escalation, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is starting evidence collection before participants share the same boundary and operating rules. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Confirm authority and introductions.
- 2. Restate scope.
- 3. Review daily cadence.
- 4. Confirm request and escalation channels.
- 5. Identify immediate constraints.
- 6. Document decisions.

Evidence to Preserve: opening agenda; attendance; action items

MSP implementation note: Keep executive remarks factual and brief. The assessment is not a sales presentation.

17.26 Treat Examine Activities as Evidence Evaluation

Policies, SSP content, configurations, logs, tickets, reports, diagrams, approvals, and provider artifacts should be presented as evidence tied to the relevant requirement and objective.

Assessment execution requires Harbor Point to provide artifacts that are relevant, attributable, current, and internally consistent. The accountable participants are the evidence lead, objective owners, document owners, and provider custodians. They should work from an evidence index linking each item to source, time period, system, objective, and release approval, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is overwhelming assessors with bulk repositories or relying on policies that do not show implementation. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Read the request.
- 2. Identify the authoritative source.
- 3. Verify scope and dates.
- 4. Remove unrelated material.
- 5. Release through the tracker.
- 6. Answer follow-up questions with version control.

Evidence to Preserve: evidence index; source references; artifact notes

MSP implementation note: Do not flood the assessor with unrelated files in hopes that volume substitutes for relevance.

17.27 Treat Interviews as Operational Verification

The assessor may use interviews to determine whether personnel understand responsibilities and perform the process as described. Contradictions should be investigated, not coached away.

Assessment execution requires Harbor Point to let interviews reveal how work is actually performed. The accountable participants are control owners, operators, supervisors, the assessment coordinator, and provider participants. They should work from interview notes and follow-up records tied to the relevant objective, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is coaching uniform scripts that collapse when the assessor asks about exceptions, frequency, or recent examples. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Answer from personal responsibility.
- 2. Distinguish policy from practice.
- 3. Show the normal record.
- 4. Acknowledge uncertainty.
- 5. Investigate contradictions.
- 6. Correct the process rather than the story.

Evidence to Preserve: interview schedule; role map; follow-up log

MSP implementation note: MSP staff should answer only within their assigned responsibility and avoid guessing about customer decisions.

17.28 Treat Tests as Controlled Verification

Tests may involve observing or exercising mechanisms and processes. Harbor Point ensures the test is authorized and that the environment remains protected.

Assessment execution requires Harbor Point to conduct tests under explicit authorization and technical safeguards. The accountable participants are the system owner, technical lead, change authority, provider operator, and assessor. They should work from a test record containing authorization, steps, timestamps, observations, artifacts, exceptions, and restoration, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is allowing an assessment test to disrupt service, expose secrets, or produce results that cannot be reproduced. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Agree the objective.
- 2. Select the system and test identity.
- 3. Define boundaries and stop conditions.
- 4. Monitor execution.
- 5. Capture results.
- 6. Restore state.
- 7. Record anomalies.

Evidence to Preserve: test record; approvals; observed result; follow-up evidence

MSP implementation note: Use named test accounts and preserve the result where appropriate.

17.29 Manage Evidence Requests with One Tracker

A single request tracker records the request, owner, due time, source, status, transfer location, clarification, and final disposition.

Assessment execution requires Harbor Point to operate one authoritative queue for all assessor requests. The accountable participants are the evidence coordinator, request

owners, quality reviewer, and assessment coordinator. They should work from a request register showing ID, exact request, objective, owner, due date, status, response, version, and closure, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is losing requests in chat and email or sending conflicting responses from multiple teams. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Log the request immediately.
- 2. Clarify ambiguity.
- 3. Assign one owner.
- 4. Review the response.
- 5. Transmit through the approved channel.
- 6. Obtain closure or record follow-up.

Evidence to Preserve: evidence request tracker; delivery log; unresolved requests

MSP implementation note: Avoid parallel private channels between individual engineers and assessors.

17.30 Use Daily Closeouts

Daily closeouts identify completed activities, open evidence requests, scope questions, schedule changes, technical issues, and next-day priorities.

Assessment execution requires Harbor Point to use daily closeouts to keep facts, work, and expectations synchronized. The accountable participants are the assessment coordinator, C3PAO lead, evidence lead, technical lead, and provider liaisons. They should work from a daily closeout record with completed work, open requests, risks, schedule changes, and next-day owners, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed

environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is allowing misunderstandings and overdue requests to compound until the final day. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Reconcile the tracker.
- 2. Clarify new issues.
- 3. Identify missing people or access.
- 4. Approve schedule adjustments.
- 5. Assign overnight actions.
- 6. Circulate a concise record.

Evidence to Preserve: daily closeout notes; action list; schedule updates

MSP implementation note: Keep closeout notes factual; do not speculate about scores or pressure the assessment team.

17.31 Control Remote Access for Assessment Activities

If assessors need remote participation or demonstrations, provide least-privilege, time-bound, monitored access appropriate to the activity.

Assessment execution requires Harbor Point to grant only the remote access needed for approved assessment activity. The accountable participants are the system owner, identity administrator, security operations, assessment coordinator, and C3PAO. They should work from an access authorization record with identity, privilege, purpose, system, start, expiration, monitoring, and removal, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is creating shared, persistent, overprivileged, or unmonitored assessor accounts. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Prefer supervised sessions.
- 2. Use named identities.
- 3. Apply least privilege and MFA.
- 4. Restrict time and network path.
- 5. Monitor use.
- 6. Remove access promptly.
- 7. Retain access logs.

Evidence to Preserve: temporary access approvals; account logs; removal evidence

MSP implementation note: Do not create permanent assessor accounts unless a documented need exists.

17.32 Coordinate MSP and MSSP Participation

NorthStar and Beacon provide evidence and explain services they perform. Harbor Point remains responsible for its CMMC representations and for explaining customer-owned processes.

Assessment execution requires Harbor Point to use providers as accountable witnesses for their assigned services. The accountable participants are the customer assessment coordinator, MSP and MSSP service owners, technical operators, and C3PAO. They should work from a participation matrix mapping each provider to objectives, evidence, interviews, demonstrations, and escalation, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is letting the MSP speak for customer governance or leaving provider-controlled mechanisms unexplained. In an MSP-supported

environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Identify shared responsibilities.
- 2. Assign customer and provider speakers.
- 3. Prepare tenant-specific records.
- 4. Rehearse handoffs.
- 5. Keep the customer present for decisions and representations.

Evidence to Preserve: provider participation matrix; interview roster; evidence ownership map

MSP implementation note: The provider should not answer “yes” for controls it does not own.

17.33 Handle Unexpected Findings Professionally

An assessor may identify a condition the readiness team missed. Harbor Point records the fact, provides relevant evidence, and avoids defensive argument or emergency evidence manufacture.

Assessment execution requires Harbor Point to respond to unexpected findings with facts and disciplined investigation. The accountable participants are the objective owner, assessment coordinator, technical lead, executive sponsor, and legal or contracts contacts when needed. They should work from an issue record separating assessor observation, verified facts, immediate risk, response, and later remediation, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is arguing reflexively, hiding the issue, or making an uncontrolled production change during assessment. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who

may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Clarify the observation.
- 2. Preserve relevant evidence.
- 3. Verify the current state.
- 4. Address urgent security risk safely.
- 5. Provide factual context.
- 6. Track remediation outside the assessment decision.

Evidence to Preserve: issue log; source evidence; corrective-action record

MSP implementation note: Do not alter production during an assessment solely to conceal the observed condition.

17.34 Preserve Assessment Integrity Under Schedule Pressure

Delays, missing personnel, provider outages, and evidence gaps can create pressure to improvise. The governance team protects safety and accuracy even if the schedule must change.

Assessment execution requires Harbor Point to protect evidence quality and safety when the schedule tightens. The accountable participants are the executive sponsor, assessment coordinator, change authority, and C3PAO lead. They should work from a schedule-risk log with tradeoffs, decisions, and authorized changes, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. During execution, speed must not displace accuracy, safety, or traceability. Every answer, artifact, interview, and test should be attributable to the real system and normal operating process.

The principal failure mode is using deadlines to justify skipped review, unsafe tests, unavailable control owners, or misleading substitutes. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Surface the constraint early.
- 2. Prioritize by assessment plan.
- 3. Add qualified support.
- 4. Negotiate documented changes.
- 5. Refuse unsafe activity.
- 6. Preserve the reason for each decision.

Evidence to Preserve: schedule deviation log; escalation decisions; change approvals

MSP implementation note: A clean delay is better than an unsafe test or misleading representation.

17.35 Separate Factual Corrections from Assessment Judgment

If the assessment record contains an incorrect hostname, date, system description, or other factual error, provide objective correction. A disagreement with an assessor's determination is different and should follow the appropriate process.

Findings and closeout requires Harbor Point to correct objective errors without trying to negotiate professional judgment. The accountable participants are the assessment coordinator, evidence lead, objective owner, legal counsel when appropriate, and C3PAO lead. They should work from a factual-correction record stating the disputed fact, accurate fact, supporting source, and requested correction, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is turning every unfavorable conclusion into an argument or mixing new remediation with evidence of the assessed state. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Identify the precise statement.
- 2. Verify the contemporaneous record.
- 3. Cite the source.
- 4. Submit through the defined channel.
- 5. Accept or escalate the resulting judgment through the proper process.

Evidence to Preserve: factual correction log; supporting artifact; disposition

MSP implementation note: Use precise language: identify the fact, show the source, avoid arguing motive.

17.36 Understand MET and NOT MET Determinations

Assessment determinations are based on the applicable objectives and evidence. An organization should understand why an objective is considered satisfied or unsatisfied without attempting to negotiate the standard itself.

Findings and closeout requires Harbor Point to manage MET and NOT MET determinations as formal assessment outcomes. The accountable participants are the executive sponsor, assessment coordinator, control owner, and C3PAO. They should work from the final objective-level results and management response record, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is treating a NOT MET as a negotiable label or treating a MET as proof that no sustainment work is needed. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Confirm the objective and evidence considered.
- 2. Correct factual errors promptly.
- 3. Identify operational risk.
- 4. Separate remediation from the assessed state.
- 5. Feed results into governance and sustainment.

Evidence to Preserve: finding record; objective mapping; cited evidence

MSP implementation note: Use the finding to improve the control even when management disagrees with the impact.

17.37 Manage Conditional Status Carefully

When the governing rule permits Conditional status, only eligible unmet requirements may be carried on an authorized POA&M and the required score/conditions must be met.

Findings and closeout requires Harbor Point to use Conditional status only when every eligibility condition is satisfied. The accountable participants are the executive sponsor, affirming official, assessment coordinator, legal counsel, and C3PAO. They should work from a formal eligibility analysis, authorized POA&M, milestones, resources, and closeout plan, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is assuming any failed requirement can be deferred or presenting planned work as implemented. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Calculate the score threshold.
- 2. Screen prohibited and higher-value requirements.
- 3. Confirm the permitted path.
- 4. Approve resources.
- 5. Establish closeout evidence and management oversight.

Evidence to Preserve: conditional-status record; eligible POA&M; affirmation; deadline tracker

MSP implementation note: Do not label ordinary internal remediation as formal CMMC POA&M closeout.

17.38 Manage the 180-Day POA&M Closeout Clock

Current CMMC rules and DFARS definitions treat Conditional Level 2 status as time-limited. Harbor Point builds a closeout plan with owners, dependencies, validation, evidence, and schedule margin.

Findings and closeout requires Harbor Point to treat the 180-day closeout period as a hard compliance deadline. The accountable participants are the executive sponsor, POA&M owner, technical owners, change management, and C3PAO. They should work from an integrated closeout schedule with milestones, testing, evidence review, and assessment booking, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is waiting to schedule closeout until remediation is complete or underestimating lead times and retesting. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Book governance checkpoints.
- 2. Reserve assessor availability.
- 3. Implement through controlled changes.
- 4. Test against the original objective.
- 5. Assemble evidence.
- 6. Conduct authorized closeout before expiration.

Evidence to Preserve: POA&M; milestone tracker; validation evidence; closeout submission

MSP implementation note: Plan to finish well before the deadline; provider lead time can consume the schedule quickly.

17.39 Use Independent Closeout Validation Where Practical

The team that performed a correction should not be the only source of confidence that the condition is fixed. Re-test the original objective and preserve evidence.

Findings and closeout requires Harbor Point to obtain credible validation before presenting corrective work for closeout. The accountable participants are the remediation owner, independent reviewer, evidence lead, and executive sponsor. They should work from an internal validation report mapped to the original NOT MET objective, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is allowing the implementer to declare closure based only on a ticket or configuration screenshot. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Reperform the relevant examine, interview, and test methods.
- 2. Verify scope and persistence.
- 3. Review exceptions.
- 4. Correct weak evidence.
- 5. Authorize submission only when the result is reproducible.

Evidence to Preserve: re-test plan; test result; reviewer approval; updated SSP

MSP implementation note: Closure should demonstrate the security outcome, not only ticket completion.

17.40 Understand Appeals and Complaints Processes

Organizations should know the C3PAO’s documented processes for appeals and complaints and distinguish those mechanisms from ordinary factual clarification.

Findings and closeout requires Harbor Point to use appeals and complaints for their intended purposes. The accountable participants are the executive sponsor, legal counsel, assessment coordinator, and the designated C3PAO or ecosystem contact. They should work from a decision record classifying the issue and preserving notices, deadlines, submissions, and outcomes, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is using an appeal to replace missing evidence or using a complaint to pressure an assessment conclusion. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Review the applicable process.
- 2. Distinguish factual correction, appeal, and conduct complaint.
- 3. Preserve the record.
- 4. Meet deadlines.
- 5. State the requested remedy.
- 6. Maintain professional communications.

Evidence to Preserve: appeals procedure; complaint procedure; correspondence; decision record

MSP implementation note: Escalation should be evidence-based and professional, not a commercial threat.

17.41 Protect Assessment Records After the Engagement

Assessment workspaces may contain sensitive security information. Apply access control, retention, legal hold, return/destruction terms, and minimum-copy principles.

Findings and closeout requires Harbor Point to retain the authoritative assessment record and dispose of unnecessary copies. The accountable participants are the records owner, security officer, legal counsel, assessment coordinator, and providers.

They should work from a retention schedule and final assessment index covering reports, evidence exchanges, decisions, access logs, and destruction confirmations, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is keeping uncontrolled evidence sets across personal drives, provider tickets, and temporary sharing locations. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Identify official records.
- 2. Apply legal and contractual retention.
- 3. Reconcile copies.
- 4. Revoke links and accounts.
- 5. Obtain provider disposition confirmation.
- 6. Preserve chain of custody.

Evidence to Preserve: retention schedule; access list; destruction/return confirmation

MSP implementation note: Remove temporary shared links and unnecessary assessment copies after closeout.

17.42 Reconcile Final Status, SPRS, and Contract Records

The internal record, assessment result, CMMC UID, SPRS status, affirmation, contract files, and executive reporting should describe the same assessed environment.

Findings and closeout requires Harbor Point to align the final result with SPRS, CMMC UID, affirmations, contracts, and management reporting. The accountable participants are the affirming official, contracts lead, assessment coordinator, executive sponsor, and system owner. They should work from a post-assessment

reconciliation signed by accountable owners, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. Closeout decisions require the same discipline as assessment preparation. The organization must separate contemporaneous evidence, factual corrections, remediation, formal status, and later sustainment.

The principal failure mode is leaving inconsistent status, dates, system identifiers, or contract representations across official and internal records. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Verify final status and dates.
- 2. Confirm the system and UID.
- 3. Update required records.
- 4. Schedule affirmation and expiration milestones.
- 5. Notify contract stakeholders.
- 6. Resolve discrepancies.

Evidence to Preserve: SPRS record; CMMC UID; certificate/status record; contract file; affirmation

MSP implementation note: Treat identifier mismatches as governance defects requiring correction.

17.43 Harbor Point Case: Selecting the C3PAO

Harbor Point compares three C3PAOs using authorization, independence, provider-heavy environment experience, secure evidence handling, staffing continuity, travel assumptions, and pricing basis. The lowest quoted price is not selected because its scope assumptions omit a remote engineering site and a key cloud service.

Harbor Point application requires Harbor Point to select a C3PAO through a documented best-value process. The accountable participants are Harbor Point procurement, the assessment coordinator, NorthStar's technical liaison, and the executive sponsor. They should work from Harbor Point's scored selection matrix and decision memorandum, because the C3PAO must be able to distinguish a

management assertion from a fact supported by the assessed environment. The Harbor Point cases show how the operating model behaves under pressure. Each case should leave behind a reusable management record, not merely a story about how one meeting was handled.

The principal failure mode is choosing on price before validating independence, staffing, evidence security, and environment fit. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Issue one scope baseline.
- 2. Conduct conflict checks.
- 3. Score capability and security.
- 4. Normalize pricing.
- 5. Interview the proposed lead.
- 6. Document the final decision.

Evidence to Preserve: selection matrix; procurement decision; scope assumptions

MSP implementation note: MSPs can help define technical complexity but should not steer the customer to an assessor based on a hidden referral arrangement.

17.44 Harbor Point Case: The Pre-Assessment Scope Conflict

During kickoff, the assessor asks about Beacon’s SIEM environment and NorthStar’s privileged support platform. Harbor Point’s first diagram does not show either dependency. The team pauses, updates the provider map, and reconciles the SSP before formal assessment activity proceeds.

Harbor Point application requires Harbor Point to resolve whether a newly identified cloud workflow belongs inside the assessment boundary. The accountable participants are Harbor Point's system owner, NorthStar's architect, contracts, and the C3PAO scope lead. They should work from a scope decision package with data-flow evidence, SSP changes, and schedule impact, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed

environment. The Harbor Point cases show how the operating model behaves under pressure. Each case should leave behind a reusable management record, not merely a story about how one meeting was handled.

The principal failure mode is pressing ahead with an assessment after discovering that CUI may traverse an undocumented service. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Pause the affected planning.
- 2. Trace the data.
- 3. Determine contractual and scoping impact.
- 4. Update the SSP and diagrams.
- 5. Remediate or revise the assessment plan.

Evidence to Preserve: updated scope diagram; SSP revision; responsibility matrix; decision log

MSP implementation note: This is why provider dependencies must be resolved before assessment week.

17.45 Harbor Point Case: An Interview Contradiction

A Harbor Point manager says terminated users are disabled immediately. NorthStar’s engineer explains that the MSP waits for an approved offboarding ticket. Rather than coaching either person, the team produces the actual process, timestamps, and sample records. The inconsistency reveals a governance gap that requires correction.

Harbor Point application requires Harbor Point to investigate conflicting interview statements against operational records. The accountable participants are Harbor Point's assessment coordinator, the interviewed supervisor, NorthStar's service owner, and the evidence lead. They should work from a contradiction-resolution record linked to tickets, procedures, and follow-up interviews, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The Harbor Point cases show how the operating model behaves under

pressure. Each case should leave behind a reusable management record, not merely a story about how one meeting was handled.

The principal failure mode is coaching participants into a shared answer instead of discovering why practice differs. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Capture each statement accurately.
- 2. Inspect recent records.
- 3. Identify role or procedure ambiguity.
- 4. Correct factual misunderstandings.
- 5. Disclose the resolved facts to the assessor.

Evidence to Preserve: interview follow-up; offboarding records; policy; corrective action

MSP implementation note: Contradictions are diagnostic information, not something to hide.

17.46 Harbor Point Case: A Safe Technical Demonstration

The assessor asks to observe privileged MFA and logging. NorthStar uses a named test administrator in Harbor Point’s tenant, generates an approved sign-in event, and Beacon traces it into the customer-specific SIEM view. No unrelated tenant data is exposed.

Harbor Point application requires Harbor Point to prove a security mechanism without risking Harbor Point production. The accountable participants are NorthStar's platform engineer, Harbor Point's technical lead, change management, and the assessor. They should work from an approved demonstration script and execution record, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The Harbor Point cases show how the operating model behaves under pressure. Each case should leave behind a reusable management record, not merely a story about how one meeting was handled.

The principal failure mode is testing with a privileged production account or changing a shared MSP policy during the assessment. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Create a named test object.
- 2. Isolate the action.
- 3. Obtain authorization.
- 4. Monitor the result.
- 5. Preserve customer-specific output.
- 6. Roll back and verify.

Evidence to Preserve: test authorization; sign-in log; SIEM event; evidence note

MSP implementation note: Design demonstrations before assessment week so safety and attribution are not improvised.

17.47 Harbor Point Case: Closing an Eligible POA&M Item

An eligible deficiency is placed on a formal POA&M under the applicable rule. Harbor Point assigns one outcome owner, NorthStar performs the change, Beacon validates monitoring, and an independent reviewer re-tests the objective. Closeout is based on evidence, not the completion date in the project tool.

Harbor Point application requires Harbor Point to close an eligible POA&M item with implementation and objective-level verification. The accountable participants are Harbor Point's POA&M owner, NorthStar's implementer, an independent reviewer, and the C3PAO. They should work from change records, operating evidence, validation results, and formal closeout documentation, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The Harbor Point cases show how the operating model behaves under pressure. Each case should leave behind a reusable management record, not merely a story about how one meeting was handled.

The principal failure mode is declaring closure when the configuration change exists but the process has not operated or been tested. In an MSP-supported environment,

this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Confirm eligibility.
- 2. Implement under change control.
- 3. Collect repeated operating evidence.
- 4. Independently test the original objective.
- 5. Submit for authorized closeout within 180 days.

Evidence to Preserve: formal POA&M; change tickets; re-test evidence; closeout decision

MSP implementation note: Keep internal project tracking and formal CMMC records linked but distinct.

17.48 Return to Continuous Readiness After the Assessment

The engagement ends, but the operating program continues. Harbor Point removes temporary access, reconciles records, captures lessons learned, updates evidence routines, and returns to the Chapter 16 sustainment cadence.

Harbor Point application requires Harbor Point to convert assessment lessons into the continuous-readiness program. The accountable participants are the executive sponsor, program owner, control owners, NorthStar, Beacon, and records management. They should work from a lessons-learned register linked to Chapter 16 metrics, calendars, triggers, and risk items, because the C3PAO must be able to distinguish a management assertion from a fact supported by the assessed environment. The Harbor Point cases show how the operating model behaves under pressure. Each case should leave behind a reusable management record, not merely a story about how one meeting was handled.

The principal failure mode is archiving the assessment without fixing the retrieval, responsibility, or control-health weaknesses it exposed. In an MSP-supported environment, this risk increases when the customer, NorthStar, and Beacon each hold only part of the explanation. Harbor Point should therefore identify who owns the decision, who operates the mechanism, who holds the authoritative record, and who

may communicate it. If those four answers do not align, the assessment coordinator should treat the issue as an open readiness risk rather than improvising during the engagement.

Recommended operating sequence:

- 1. Remove temporary access.
- 2. Reconcile evidence.
- 3. Analyze recurring friction.
- 4. Assign systemic improvements.
- 5. Update readiness measures.
- 6. Brief management.
- 7. Verify completion in the next quarterly review.

Evidence to Preserve: lessons learned; access cleanup; evidence updates; annual affirmation calendar

MSP implementation note: The best sign of a mature assessment is that ordinary operations remain disciplined after the assessors leave.

C3PAO Engagement Field Guide

The following field guide is designed for the customer assessment coordinator and provider liaisons. It is a practical operating aid, not an additional CMMC requirement. Use it at three points: when comparing C3PAOs, during the formal kickoff and scope reconciliation, and at the end of each assessment day. The guide is most effective when its entries point to actual owners and records rather than generic statements of intent.

Phase	Customer Lead	MSP/MSSP Role	C3PAO Boundary	Key Output
Before selection	Confirm contractual path, scope stability, budget, timing	Describe environment and provider dependencies	No formal assessment role yet	Assessment decision package
Selection	Verify authorization, fit, independence, evidence security, commercial terms	Provide technical complexity input	Remain independent of implementation interests	Selection record
Contracting	Execute SOW, security terms,	Commit provider participation and	Define assessment services without	Signed

Phase	Customer Lead	MSP/MSSP Role	C3PAO Boundary	Key Output
	schedule, change control	evidence delivery	outcome guarantee	engagement
Pre-assessment	Reconcile SSP, scope, people, logistics, evidence channels	Validate provider inventory, evidence, demonstrations	Review planned assessment logistics	Ready assessment baseline
Assessment	Coordinate examine/interview/test; control requests	Answer provider-owned questions; demonstrate services	Make independent determinations	Assessment record
Closeout	Handle factual corrections, POA&M actions, appeals as appropriate	Implement assigned corrections and evidence	Report results and closeout according to process	Final or conditional status
Post-assessment	Remove temporary access, reconcile records, sustain controls	Resume normal evidence and service cadence	Retain/handle records per governing process	Continuous readiness

Implementation Checklist

- ☐ Confirm the required CMMC level and assessment pathway from the actual solicitation or contract.
- ☐ Check current Department implementation notices before committing to a certification schedule.
- ☐ Freeze the assessment baseline only after major scope and provider questions are resolved.
- ☐ Verify the C3PAO's current authorization/standing and document the date checked.
- ☐ Perform an independence/conflict review for the C3PAO and any related consulting relationships.
- ☐ Compare pricing assumptions, not only total quoted price.
- ☐ Define secure evidence transfer, storage, retention, return, and destruction terms.

- ☐ Define staffing, substitutions, travel, locations, remote participation, and change-control rules.
- ☐ Create an internal governance roster with executive sponsor, coordinator, technical lead, evidence lead, and provider liaisons.
- ☐ Reconcile SSP, diagrams, asset categories, locations, cloud services, specialized assets, SPAs, and ESPs.
- ☐ Create a customer/provider participation matrix for interviews, demonstrations, and evidence.
- ☐ Create a single evidence-request tracker and one authoritative communications channel.
- ☐ Prepare safe technical demonstrations using named test objects and customer-specific views.
- ☐ Protect unrelated tenants and secrets when provider evidence comes from multi-tenant platforms.
- ☐ Use daily closeouts to manage open requests, scope issues, schedule changes, and technical problems.
- ☐ Record factual corrections separately from disputes over assessment judgment.
- ☐ If Conditional status applies, validate formal POA&M eligibility and track the 180-day closeout requirement.
- ☐ Re-test corrections against the original objective and preserve closure evidence.
- ☐ Understand the C3PAO's appeal and complaint processes before the assessment begins.
- ☐ Reconcile final assessment status, CMMC UID, SPRS records, affirmation, contracts, and executive reporting.
- ☐ Remove temporary assessor access and assessment-only sharing after closeout.
- ☐ Capture lessons learned and feed them into the continuous-readiness cadence from Chapter 16.

Operational Workshops

Workshop 1 - C3PAO Selection Matrix

Compare at least three candidate C3PAOs using authorization status, independence, relevant environment experience, evidence security, staffing, schedule, pricing assumptions, and change-control terms. Document why the selected organization fits the planned assessment rather than simply choosing the lowest price.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 2 - Conflict-of-Interest Review

Map every consulting, referral, implementation, reseller, and business relationship among the customer, MSP, consultants, and proposed C3PAO. Identify relationships that could create actual or perceived conflicts and determine how they will be avoided or disclosed.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 3 - Scope Reconciliation Session

Walk through the SSP, network/data-flow diagrams, asset inventory, locations, cloud services, remote work, SPAs, specialized assets, and external providers. Produce a signed internal baseline of what the organization intends to present for assessment.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 4 - Evidence Exchange Dry Run

Select ten high-value artifacts and move them through the planned secure transfer process. Confirm permissions, attribution, tenant filtering, timestamps, readability, and retention. Record any transfer or labeling failure.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 5 - Interview Readiness Exercise

Choose five real control owners. Ask each to explain the trigger, action, approval, evidence, exception path, and provider dependency for a process they actually perform. Correct misunderstandings in the operating process rather than scripting answers.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 6 - Safe Technical Demonstration

Design and execute a controlled demonstration for privileged MFA, log generation, account disablement, or another mechanism. Define test object, authorization, expected result, evidence, rollback, and production safeguards.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 7 - Multi-Tenant Evidence Protection

Take one MSP platform that serves multiple customers. Design a method to prove Harbor Point's configuration and operations without exposing other customer records. Test redaction, filtering, screenshots, exports, and live demonstration options.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 8 - Daily Closeout Simulation

Run a mock assessment day with evidence requests, a scope question, an unavailable interviewee, and one technical-test problem. Conduct a 20-minute closeout and produce the next-day action list.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 9 - Factual Correction vs Appeal

Review six sample disputes. Classify each as a factual correction, evidence supplement, professional disagreement, appeal, complaint, or ordinary remediation issue. Draft the appropriate response channel for each.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Workshop 10 - Post-Assessment Cleanup

Inventory all temporary accounts, shared links, exported evidence packages, local copies, test objects, and special firewall or access rules created for assessment. Build the closure checklist and assign retention or destruction decisions.

Deliverable: a completed workshop record with owner, participants, assumptions, observed result, identified gap, corrective action, and evidence location.

Working Templates

C3PAO Selection Record

Field	Record
Candidate C3PAO	_____ ___
Authorization checked/date	_____

Field	Record
	___
Independence concerns	_____ ___
Relevant environment experience	_____ ___
Lead assessor/staffing assumptions	_____ ___
Evidence-security method	_____ ___
Locations/travel	_____ ___
Schedule	_____ ___
Pricing assumptions	_____ ___
Change-order terms	_____ ___
Reference checks	_____ ___
Selection decision/approver	_____ ___

Assessment Governance Roster

Field	Record
Executive sponsor	_____ ___
Assessment coordinator	_____ ___
Backup coordinator	_____ ___
Technical lead	_____ ___
Evidence coordinator	_____

Field	Record
	___
Legal/contract contact	_____ ___
Facilities contact	_____ ___
NorthStar liaison	_____ ___
Beacon liaison	_____ ___
Cloud/provider contacts	_____ ___
Emergency escalation path	_____ ___

Evidence Request Record

Field	Record
Request ID	_____ ___
Requirement/objective	_____ ___
Requested artifact or demonstration	_____ ___
Requesting assessor	_____ ___
Owner	_____ ___
Authoritative source	_____ ___
Customer/tenant	_____ ___
Time period	_____ ___
Due date/time	_____

Field	Record
	___
Transfer location	_____ ___
Clarification	_____ ___
Delivered by/date	_____ ___
Disposition	_____ ___

Daily Assessment Closeout

Field	Record
Date	_____ ___
Activities completed	_____ ___
Open evidence requests	_____ ___
Open scope questions	_____ ___
Interview follow-ups	_____ ___
Technical test issues	_____ ___
Schedule changes	_____ ___
Provider dependencies	_____ ___
Safety/security concerns	_____ ___
Decisions needed	_____ ___
Next-day priorities	_____

Field	Record
	___

Factual Correction Record

Field	Record
Assessment reference	_____ ___
Observed statement	_____ ___
Fact believed incorrect	_____ ___
Authoritative source	_____ ___
Supporting evidence	_____ ___
Submitted by/date	_____ ___
C3PAO disposition	_____ ___
Final record update	_____ ___

Post-Assessment Cleanup Record

Field	Record
Temporary accounts	_____ ___
Remote access	_____ ___
Shared links	_____ ___
Assessment workspace	_____ ___
Local evidence copies	_____

Field	Record
	___
Test data/accounts	_____ ___
Temporary rules/configurations	_____ ___
Retention decision	_____ ___
Return/destruction evidence	_____ ___
Owner/date completed	_____ ___

Review Questions

1. What distinguishes a C3PAO from an MSP or compliance consultant?
2. Why should the contractual assessment pathway be confirmed before engaging a C3PAO?
3. How can changing CMMC implementation schedules affect assessment planning?
4. Why should scope be stabilized before requesting firm commercial proposals?
5. What is the difference between a readiness review and a certification assessment?
6. Why is assessor independence important?
7. Which internal governance roles should be assigned before the engagement?
8. What does a defensible definition of assessment success look like?
9. How should an organization verify a C3PAO's current status?
10. Why should environment-specific experience be considered during selection?
11. What evidence-security questions should be addressed in the contract?
12. Why does assessment-team staffing continuity matter?
13. Which factors commonly drive C3PAO pricing?
14. Why are outcome-based commercial terms inappropriate?
15. What should the assessment statement of work define?
16. Why should change control be agreed before work starts?
17. What should be accomplished during the engagement kickoff?

18. How should the customer reconcile assessment scope with the C3PAO?
19. Why are unresolved external-provider scope questions dangerous?
20. What should an evidence exchange plan contain?
21. How can an MSP protect unrelated tenants while supporting an assessment?
22. Who should participate in interviews?
23. How should technical demonstrations be made safe?
24. Why can a broad change freeze be counterproductive?
25. What is the purpose of the opening assessment session?
26. How should examine activities be supported?
27. Why should interview contradictions be investigated rather than coached away?
28. What controls should surround technical tests?
29. Why should evidence requests be managed in one tracker?
30. What is the value of daily assessment closeouts?
31. How should remote assessor access be controlled?
32. What is the correct boundary for MSP/MSSP participation?
33. How should the organization react to an unexpected finding?
34. Why is schedule pressure a risk to assessment integrity?
35. What is the difference between a factual correction and an appeal?
36. How should MET and NOT MET determinations be treated operationally?
37. When can Conditional status and a formal POA&M be relevant?
38. Why should the 180-day closeout requirement be treated as a hard management constraint?
39. What records should be reconciled after the assessment?
40. What lessons from the Harbor Point cases should be fed back into continuous readiness?

Answer Guidance

Questions 1 through 8 focus on roles, independence, assessment pathway, and governance. The organization should enter the engagement knowing what the C3PAO is authorized to do, what the customer remains accountable for, and how the MSP supports but does not replace the customer.

Questions 9 through 16 focus on selection and contracting. Strong engagements verify authorization, fit, evidence security, staffing, pricing assumptions, and change control while avoiding commercial terms that could pressure assessment judgment.

Questions 17 through 24 focus on pre-assessment alignment. Scope, evidence channels, provider participation, interviews, demonstrations, and change coordination should be resolved before assessment pressure makes those decisions harder.

Questions 25 through 34 focus on execution. Evidence should be relevant and traceable, interviews should reflect real operations, tests should be controlled, requests should be tracked, and schedule pressure should never justify unsafe or misleading behavior.

Questions 35 through 40 focus on closeout and sustainment. Factual corrections, assessment judgments, Conditional status, formal POA&M closeout, SPRS records, temporary access cleanup, and lessons learned each have distinct purposes and should be managed accordingly.

Key Terms

Term	Working meaning
C3PAO	A CMMC Third-Party Assessment Organization authorized within the CMMC ecosystem to conduct applicable Level 2 certification assessments.
Assessment Coordinator	The customer role that manages schedule, participants, evidence requests, logistics, and internal escalation for the engagement.
Lead Assessor	The qualified assessment professional responsible for leading the assessment team and assessment activities under the applicable process.
Impartiality	Freedom from commercial, implementation, personal, or organizational influence that could compromise independent assessment judgment.
Conflict of Interest	A relationship or circumstance that could impair, or reasonably appear to impair, objective assessment activity.
Examine	Assessment method involving review of specifications, mechanisms, records, artifacts, configurations, or other evidence.
Interview	Assessment method involving discussion with

Term	Working meaning
	personnel who perform, manage, or oversee relevant activities.
Test	Assessment method involving exercising or observing mechanisms, processes, or activities to determine whether the required outcome occurs.
Factual Correction	A documented correction to an objective fact in the assessment record, supported by authoritative evidence.
Appeal	A formal request for review of an assessment-related decision through the applicable documented process.
Complaint	A formal expression of dissatisfaction handled through the applicable complaint process, distinct from ordinary technical clarification.
Conditional CMMC Status	A time-limited CMMC status available under specified conditions when eligible unmet requirements are carried on an authorized POA&M.
CMMC UID	The unique identifier associated with a CMMC assessment/status record in SPRS for a contractor information system.
Evidence Custodian	The person or role responsible for maintaining and producing an authoritative evidence source.
Assessment Workspace	A controlled repository or collaboration area used to stage or exchange assessment evidence.
Daily Closeout	A short governance meeting used to reconcile completed activities, open requests, scope questions, schedule changes, and next steps.

Chapter Closing

A C3PAO engagement should not feel like an organization temporarily becoming someone else for assessment week. A defensible assessment posture is the opposite: the environment, responsibilities, evidence, and people presented to the assessor are the same ones used in ordinary operations. The customer can explain why a control

exists, who owns it, how it is performed, what happens when it fails, and where the authoritative record is kept.

For MSP-supported organizations, this requires disciplined boundaries. Harbor Point owns its contractual and CMMC representations. NorthStar and Beacon are accountable for the services, configurations, records, and explanations within their assigned responsibilities. The C3PAO independently evaluates conformity. When those boundaries are clear, the assessment becomes more efficient because participants do not spend time deciding who is allowed to answer, which artifact is authoritative, or whether the provider can speak for the customer.

The engagement also produces information that should improve the operating program. Evidence requests reveal weak retrieval paths. Interview contradictions reveal process ambiguity. Technical tests expose fragile assumptions. Findings reveal control weaknesses. Even a successful assessment can identify ways to reduce future effort. Those lessons should return to the continuous-readiness model from Chapter 16 rather than disappearing into an archived assessment folder.

The practical standard is therefore not performance. It is transparency, control, and continuity. An organization that can work effectively with an independent C3PAO without changing its story, hiding its providers, or manufacturing evidence has reached a meaningful level of operational maturity.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Use the current text for assessment types, CMMC status, POA&M, affirmation, scoping, external service providers, and ecosystem roles.

R2. Department CMMC Resources & Documentation. Current CMMC program resources, assessment guides, scoping guides, and implementation notices. https://dodcio.defense.gov/CMMC/Resources-Documentation/

R3. Department CMMC About / implementation notice. On July 13, 2026, the Department announced immediate suspension of CMMC Phase II requirements while Phase I self-assessment requirements remain in place. https://dodcio.defense.gov/CMMC/About/

R4. Acquisition.gov. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (Nov. 2025). Includes current-status, maintenance, annual affirmation, CMMC UID, SPRS, POA&M closeout, and flowdown requirements when the clause applies.

https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements.

R5. Department CMMC Level 2 Assessment Guide and related Level 2 documentation available through the current CMMC Resources & Documentation page. Use the edition applicable to the assessment being planned.

R6. The Cyber AB. Current CMMC ecosystem requirements, C3PAO listings/status, professional qualification information, assessment-process resources, and applicable policies. Verify current documents at the time of engagement.

R7. NIST SP 800-171 Revision 2 and NIST SP 800-171A (June 2018), as incorporated into the published CMMC Level 2 assessment framework discussed throughout this book. Use current contractual and CMMC sources to determine the applicable baseline.

R8. Applicable solicitation, contract, subcontract, statement of work, security addendum, and legal/contractual guidance for the specific organization. These sources determine the organization's actual obligations and should be reviewed before scheduling a formal assessment.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance. It does not replace governing regulations, contract clauses, current Department implementation guidance, Cyber AB requirements, legal advice, or an authorized CMMC assessment determination.

CMMC for MSPs

From Readiness to Certification

Chapter 18

Assessment Day: What MSPs Should Expect

By Dr. Charles Edwards

Detailed edition • September 2026

Chapter Focus

How an MSP-supported organization conducts itself during a CMMC Level 2 certification assessment: opening meeting, evidence examination, interviews, technical demonstrations, sampling, request tracking, missing evidence, assessor questions, daily closeout, findings, and controlled provider participation.

Chapter Contents

- Purpose, learning objectives, current source context, and assessment-day operating principles
- 18.1–18.8 Opening the assessment, confirming the operating model, scope, schedule, and communications
- 18.9–18.16 Examine, interview, and test methods; interview readiness and provider participation
- 18.17–18.28 Evidence examination, technical demonstrations, sampling, remote assessment, and multi-tenant safeguards
- 18.29–18.38 Missing evidence, conflicting evidence, findings, factual corrections, scope changes, and daily closeout
- 18.39–18.48 Harbor Point assessment-week scenarios, executive communications, provider coordination, and lessons learned
- Assessment-day field guide, implementation checklist, operational workshops, working templates, review questions, key terms, and official references

Chapter Purpose

Chapter 17 explained how Harbor Point selects and works with a C3PAO before the formal assessment begins. Chapter 18 moves into the assessment itself. This is the period when planning becomes observable behavior. The organization must show what is implemented, explain how the environment actually operates, produce authoritative records, and allow the assessment team to examine, interview, and test the practices that apply to the defined scope. The MSP is often central to this process because many of the relevant systems, configurations, logs, tickets, monitoring activities, and administrative workflows are operated or supported by the provider.

Assessment day should not be treated as a performance. An organization that attempts to stage a different environment, rehearse artificial answers, reconstruct historical evidence, or hide operating exceptions creates more risk, not less. Assessors are evaluating implementation across people, process, and technology. A polished screenshot may be useful, but it cannot substitute for a process that is understood by responsible personnel, consistently executed, reflected in system state, and supported by records from the period being assessed.

For the MSP, the key challenge is disciplined participation. NorthStar should be ready to explain the services it actually performs for Harbor Point, retrieve customer-specific evidence, demonstrate technical settings safely, and answer questions about its own operating procedures. It should not take over customer interviews, answer questions outside its responsibility, expose other tenants, or attempt to negotiate assessment conclusions. Beacon can explain detection, triage, escalation, and monitoring evidence, but Harbor Point must still explain its own management decisions, approvals, incident responsibilities, and contractual representations.

This chapter treats assessment day as an operational workflow rather than a ceremonial event. It covers the opening meeting, scope confirmation, communications, examine/interview/test methods, interview preparation, evidence examination, technical demonstrations, sampling, remote assessment, multi-tenant security, missing or contradictory evidence, factual corrections, potential findings, daily internal closeout, executive communication, and post-day lessons. The objective is to make the real environment understandable without turning the assessment into theater.

Learning Objectives

- Explain the purpose and structure of the opening meeting and the assessment-day chain of communication.

- Distinguish the examine, interview, and test assessment methods and explain why multiple methods may be used for the same requirement.
- Prepare customer and provider interviewees to explain real responsibilities without scripting or coaching artificial answers.
- Operate an evidence-request workflow that is fast, traceable, customer-specific, and secure.
- Plan and execute technical demonstrations using controlled test objects, least privilege, logging, and customer-scoped views.
- Protect other customers and provider-sensitive data when the supporting MSP uses multi-tenant platforms.
- Respond correctly when evidence is missing, contradictory, stale, or inconsistent with documented procedures.
- Manage factual corrections, potential findings, scope questions, and daily closeout without interfering with assessor independence.
- Coordinate executives, IT staff, security staff, MSP personnel, MSSP personnel, and other providers throughout assessment week.
- Convert assessment-day friction into durable improvements in MSP service delivery and continuous readiness.

Current Source Context - September 2026

The Level 2 certification assessment process remains defined in the CMMC program rule and related assessment guidance. The published Level 2 assessment model relies on the established NIST SP 800-171 Revision 2 requirements and assessment objectives referenced by the CMMC program. Organizations should always use the current governing rule, contract clause, DoD implementation notice, and authorized C3PAO instructions that apply to the specific engagement.

As of September 20, 2026, DoD has suspended the planned CMMC Phase II implementation that had been scheduled for November 10, 2026. Phase I self-assessment requirements remain in place, and the Department has announced a broader CMMC review. This timing change affects rollout and contract implementation; it does not make the assessment-day operating disciplines in this chapter irrelevant. Organizations may still prepare for future certification assessments, may have contractual cybersecurity obligations independent of certification timing, and should avoid representing internal readiness work as a completed C3PAO certification assessment.

This chapter therefore distinguishes between formal program requirements and recommended operating practices. Request trackers, interview schedules, evidence-

room conventions, daily closeout records, demonstration plans, and provider coordination boards are practical management methods. They should not be described as additional CMMC requirements unless the governing rule, contract, or authorized assessment procedure specifically requires them.

18.1 Treat Assessment Day as Verification, Not Performance

Treat Assessment Day as Verification, Not Performance is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. The assessment should reveal the environment that exists in normal operations. Harbor Point should not activate temporary controls merely for the assessor, and NorthStar should not create a special customer state that disappears after the assessment. The safest operating rule is simple: present the real system, real workflow, real records, and real responsible personnel.

For Harbor Point Engineering, the practical question is not whether someone can produce a polished answer on demand. The question is whether Harbor Point, NorthStar, Beacon, and any other provider can consistently explain the same responsibility boundary from their own perspective and support that explanation with current, authoritative records. The customer owns the representation of its environment. The provider owns the accuracy of the services, configurations, records, and actions it performs within the assigned boundary.

The operating risk appears when the team confuses speed with improvisation. Assessment week moves quickly, so organizations are tempted to answer from memory, create one-off screenshots without context, forward unreviewed exports, or let the most technically confident person answer every question. That approach may seem efficient, but it often creates contradictions. A controlled process assigns an owner, uses the source of truth, preserves the original request, and records exactly what was delivered.

The MSP should also remember that evidence quality and service quality are connected. If NorthStar cannot retrieve a Harbor Point-specific record without manually reconstructing it, that is an operational design weakness even if the underlying control is functioning. If Beacon can show that an alert was generated but cannot show how it was assigned and escalated to Harbor Point, the service boundary is incomplete from an assessment perspective. The assessment therefore exposes not only compliance gaps but also weaknesses in service observability.

Useful evidence for this topic includes assessment charter, current SSP, operating records, normal configurations, evidence history. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative

system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

A useful self-check is whether a qualified backup person could reproduce the same result from authoritative systems after the primary engineer leaves the room. If the answer depends on one person remembering where a file was stored, manually rebuilding history, or using an undocumented administrator shortcut, the operating model is too fragile for sustained readiness.

MSP implementation note: Keep provider participation customer-specific, traceable, and limited to the responsibility the provider actually performs. Make the real operating model easier to verify; do not create assessment-only theater.

18.2 Establish the Assessment-Day Command Structure

Establish the Assessment-Day Command Structure is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Harbor Point needs one assessment coordinator, backups, clearly identified decision makers, and a controlled path for provider participation. The command structure should solve scheduling and logistics problems without filtering technical truth or controlling assessor conclusions. NorthStar and Beacon should know who can authorize access, demonstrations, scope clarifications, and evidence transfer.

Useful evidence for this topic includes role matrix, contact list, escalation tree, decision authority, provider contacts. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.3 Use the Opening Meeting to Confirm Shared Understanding

Use the Opening Meeting to Confirm Shared Understanding is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. The opening meeting should confirm purpose, scope, schedule, locations, participants, communication methods, evidence handling, daily cadence, and known constraints. It is the last clean opportunity to identify a mismatch between the engagement assumptions and the actual environment before the assessment accelerates.

Useful evidence for this topic includes opening agenda, attendance record, scope statement, schedule, communication plan. These examples are practical methods

rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.4 Reconfirm the Assessment Boundary Before Evidence Review

Reconfirm the Assessment Boundary Before Evidence Review is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. The assessment team should be evaluating the environment described in the authorized scope. Harbor Point, NorthStar, and the C3PAO should reconcile facilities, networks, cloud services, remote access, security protection assets, external service providers, and any specialized assets that affect the assessment boundary.

Useful evidence for this topic includes network diagrams, asset inventory, data-flow diagrams, ESP list, boundary description. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.5 Reconcile CAGE, Organizational, and System Identifiers

Reconcile CAGE, Organizational, and System Identifiers is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Administrative identifiers must match the organization and environment being assessed. Small inconsistencies can create large downstream confusion when records, certificates, CMMC UIDs, contracts, or provider documentation refer to different entities or system names.

Useful evidence for this topic includes CAGE information, legal entity records, assessment scope identifiers, system names, contract references. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.6 Run One Authoritative Assessment Calendar

Run One Authoritative Assessment Calendar is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates.

Interviews, demonstrations, evidence reviews, provider availability, executive sessions, and backup windows should live on one authoritative calendar. Parallel private calendars are a common source of missed interviews and unavailable provider engineers.

Useful evidence for this topic includes master calendar, participant availability, provider dependencies, backup sessions, location links. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.7 Maintain a Controlled Assessment Communications Channel

Maintain a Controlled Assessment Communications Channel is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Assessment communications should be fast but disciplined. Harbor Point should maintain an agreed channel for logistics and request status while keeping sensitive evidence in approved repositories rather than casual chat. NorthStar should avoid side-channel commitments that bypass the customer coordinator.

Useful evidence for this topic includes communications plan, approved channels, contact roster, escalation rules, evidence-transfer instructions. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.8 Operate a Real-Time Evidence Request Tracker

Operate a Real-Time Evidence Request Tracker is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Every request should be captured with the exact request text, owner, authoritative source, scope, requested time period, delivery method, status, and follow-up. The tracker is not evidence itself; it is the operational control that prevents requests from disappearing or being answered inconsistently.

Useful evidence for this topic includes evidence tracker, timestamps, owner assignments, delivery records, follow-up notes. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of

record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.9 Understand Examine, Interview, and Test as Complementary Methods

Understand Examine, Interview, and Test as Complementary Methods is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. An assessor may examine documents and system records, interview responsible personnel, and test or observe mechanisms. These methods answer different questions. Examine shows what exists, interview shows how people understand and perform the process, and test shows how the mechanism behaves.

Useful evidence for this topic includes policies, procedures, logs, interviews, test outputs, configuration records. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.10 Expect Assessment Sequencing to Change

Expect Assessment Sequencing to Change is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A well-planned schedule is necessary, but assessors may change sequence because one artifact creates a new question or a participant becomes unavailable. Harbor Point should be able to re-sequence activities without losing control of evidence ownership or provider dependencies.

Useful evidence for this topic includes updated schedule, dependency list, reassignment notes, request tracker, participant roster. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.11 Prepare Interviewees to Explain the Real Process

Prepare Interviewees to Explain the Real Process is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates.

Preparation means ensuring that responsible personnel know their role, the systems they use, where records live, and how exceptions are handled. It does not mean giving them memorized sentences. Natural variation in wording is acceptable when the underlying process is consistent.

Useful evidence for this topic includes role descriptions, procedures, training records, interview schedule, responsibility matrix. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.12 Keep Customer and Provider Interview Responsibilities Separate

Keep Customer and Provider Interview Responsibilities Separate is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. NorthStar should answer questions about services NorthStar operates; Harbor Point should answer questions about Harbor Point decisions, approvals, business processes, and representations. A provider speaking beyond its authority can create contradictions and make the customer appear not to understand its own program.

Useful evidence for this topic includes customer responsibility matrix, service descriptions, RACI, interview assignments, escalation paths. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.13 Prepare Executives for Governance Questions

Prepare Executives for Governance Questions is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Executives may need to explain governance, risk acceptance, resources, accountability, affirmation, contract obligations, and management oversight. They do not need to recite firewall syntax, but they must be able to demonstrate that cybersecurity responsibilities are understood and governed.

Useful evidence for this topic includes governance minutes, risk decisions, approval records, policy ownership, management review evidence. These examples are

practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.14 Prepare Technical Staff for Configuration and Operations Questions

Prepare Technical Staff for Configuration and Operations Questions is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. System administrators, engineers, and security personnel should be able to show how technical settings are implemented, changed, monitored, and validated. The strongest answer connects the written requirement to the actual system state and the record created by normal operations.

Useful evidence for this topic includes configuration baselines, change tickets, screenshots, exports, logs, validation results. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.15 Prepare Service Desk and Operational Personnel

Prepare Service Desk and Operational Personnel is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Service desk and operations staff often reveal whether documented processes are real. They may be asked how access requests, terminations, incidents, changes, exceptions, or user problems are handled in practice. Their answers should align with the workflow records the organization already maintains.

Useful evidence for this topic includes tickets, queues, escalation procedures, approvals, SLA records, closure evidence. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.16 Use Follow-Up Interviews to Clarify, Not Repair

Use Follow-Up Interviews to Clarify, Not Repair is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A follow-up interview can clarify an ambiguous answer or connect evidence to the right owner. It should not be used to coach a different story after the original answer created concern. If the first answer revealed a real gap, preserve the fact and handle it through the appropriate assessment and remediation process.

Useful evidence for this topic includes interview notes, clarification records, supporting evidence, issue log, corrective action record. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.17 Present Documentary Evidence in Context

Present Documentary Evidence in Context is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Policies, procedures, SSP sections, plans, and standards are useful only when they describe the assessed environment accurately. Harbor Point should avoid dumping large libraries of documents without identifying the relevant section, owner, approval state, and relationship to actual operations.

Useful evidence for this topic includes approved policies, procedures, SSP excerpts, document metadata, approval history. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.18 Use Configuration Evidence to Show Implemented State

Use Configuration Evidence to Show Implemented State is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Configuration evidence should prove the customer-specific state, not merely show that a product has a capability. The evidence should identify tenant or system, relevant setting, population or scope, time period, and where possible the authoritative export rather than only a cropped screenshot.

Useful evidence for this topic includes configuration exports, tenant identifiers, policy assignments, system reports, screenshots with context. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.19 Use Logs and Tickets as Operational Evidence

Use Logs and Tickets as Operational Evidence is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Logs and tickets often provide stronger evidence than narrative because they show what happened over time. NorthStar and Beacon should be able to retrieve customer-specific records that connect event, action, owner, timestamp, and outcome.

Useful evidence for this topic includes SIEM records, EDR events, PSA tickets, change tickets, identity logs, alert histories. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.20 Distinguish Point-in-Time Evidence from Sustained Evidence

Distinguish Point-in-Time Evidence from Sustained Evidence is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A current setting can prove present state, but some requirements depend on recurring execution. Harbor Point should be ready to show historical records for reviews, monitoring, training, vulnerability management, account lifecycle, incidents, and other recurring activities.

Useful evidence for this topic includes historical reports, recurring review logs, prior tickets, trend records, review attestations. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.21 Show Population Coverage Before Relying on Samples

Show Population Coverage Before Relying on Samples is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Before a sample is meaningful, the organization should understand the population from which it is drawn. NorthStar should be able to identify the complete set of Harbor Point endpoints, accounts, policies, repositories, or tickets relevant to the request and then support any assessor-selected sample.

Useful evidence for this topic includes population export, inventory, account list, device list, policy assignment list, sample mapping. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.22 Preserve Sampling Independence

Preserve Sampling Independence is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. The organization may help locate records, but it should not silently curate only the cleanest items when the assessor requests a sample. If the assessor selects items, Harbor Point and NorthStar should retrieve those items faithfully and explain exceptions rather than replacing them with better examples.

Useful evidence for this topic includes sample request, population list, selected items, retrieval history, exception notes. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.23 Design Technical Demonstrations Before They Are Needed

Design Technical Demonstrations Before They Are Needed is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A demonstration should identify purpose, system, responsible operator, test object, expected behavior, evidence capture, rollback, and cleanup. Preplanning reduces risk without staging a false result. The demonstrated control should still be the real control used in normal operations.

Useful evidence for this topic includes demonstration plan, test object, operator assignment, expected result, rollback and cleanup record. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.24 Use Controlled Test Objects Where Practical

Use Controlled Test Objects Where Practical is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Creating a dedicated test account, test file, test alert, or controlled configuration change can demonstrate behavior without risking production data. The test should be clearly labeled and should not create ambiguity about historical compliance.

Useful evidence for this topic includes test account, test file, generated alert, controlled ticket, captured result, cleanup evidence. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.25 Control Privileged Access During Demonstrations

Control Privileged Access During Demonstrations is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Assessment demonstrations may require privileged consoles. Harbor Point and NorthStar should use named accounts, least privilege, time-bounded access, logging, screen control, and post-session cleanup. Credentials should never be placed in evidence packages or meeting chat.

Useful evidence for this topic includes privileged access record, temporary role assignment, session log, approval, access removal confirmation. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.26 Protect Multi-Tenant Platforms During Assessment

Protect Multi-Tenant Platforms During Assessment is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. An MSP must demonstrate Harbor Point controls without exposing other customers. Customer filters, dedicated views, redaction, controlled exports, and assessor observation of customer-scoped consoles can preserve both evidence quality and tenant confidentiality.

Useful evidence for this topic includes customer filters, tenant-scoped reports, redacted exports, access controls, demonstration screenshots. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.27 Manage Remote Assessment Logistics Deliberately

Manage Remote Assessment Logistics Deliberately is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Remote assessments add risks involving screen sharing, recording, file transfer, timezone coordination, session links, bandwidth, and privileged-console visibility. Remote convenience should not weaken evidence handling or identity verification.

Useful evidence for this topic includes remote-session plan, approved platform, participant list, file-transfer method, session schedule, access records. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.28 Handle On-Site Assessment Logistics Without Disrupting Operations

Handle On-Site Assessment Logistics Without Disrupting Operations is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. On-site work may require secure rooms, visitor controls, escort procedures, workstation access, physical demonstrations, and quiet interview space. The logistics team should support the assessor while preserving physical security and normal business operations.

Useful evidence for this topic includes visitor logs, room plan, escort assignments, physical access records, facility map, workstation plan. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.29 Respond to Missing Evidence Without Manufacturing It

Respond to Missing Evidence Without Manufacturing It is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. If requested evidence does not exist, the organization should say so. It can identify alternate authoritative evidence that genuinely supports the objective, but it should not recreate a historical record and present it as if it existed at the time.

Useful evidence for this topic includes request record, alternate evidence, gap record, corrective action ticket, management note. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.30 Resolve Contradictory Evidence by Preserving the Contradiction

Resolve Contradictory Evidence by Preserving the Contradiction is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. When the SSP says one thing and the system shows another, the discrepancy itself is important. Harbor Point should determine which record is authoritative, explain the cause, preserve the historical fact, and avoid silently changing documents during the assessment to erase the conflict.

Useful evidence for this topic includes SSP version history, system export, change record, discrepancy log, corrective action. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.31 Distinguish an Evidence Gap from an Implementation Gap

Distinguish an Evidence Gap from an Implementation Gap is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. An evidence gap means the control may exist but the organization cannot currently substantiate it adequately. An implementation gap means the required practice is not actually satisfied. The distinction matters, but the organization should not label every weakness an evidence problem merely because the control was intended to exist.

Useful evidence for this topic includes system state, historical records, procedure, interview notes, validation results. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.32 Use Factual Corrections Precisely

Use Factual Corrections Precisely is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A factual correction should identify an inaccurate fact, provide concise authoritative evidence, and explain why the correction matters. It is not an essay arguing that the assessor should overlook a weakness. The strongest correction is narrow, traceable, and supported by records that existed or accurately represent the assessed state.

Useful evidence for this topic includes factual correction form, authoritative export, ticket timestamps, logs, version history. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.33 Treat Potential Findings as Controlled Work, Not a Crisis

Treat Potential Findings as Controlled Work, Not a Crisis is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. When a potential issue emerges, the internal team should capture the fact, affected system or population, owner, supporting evidence, and immediate operational risk. Emotional debate and frantic untracked changes make the situation harder to understand.

Useful evidence for this topic includes issue log, evidence package, owner assignment, risk note, remediation ticket. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.34 Do Not Remediate in a Way That Destroys Assessment Evidence

Do Not Remediate in a Way That Destroys Assessment Evidence is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Some weaknesses can be corrected quickly, but the original state must remain understandable. Before changing a setting or closing an account, preserve the evidence needed to explain what the assessor observed and what changed afterward.

Useful evidence for this topic includes before-and-after exports, change ticket, timestamped screenshots, approval, validation result. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.35 Escalate Scope Changes Immediately

Escalate Scope Changes Immediately is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. If assessment activity reveals an unrecognized CUI flow, remote administration path, provider dependency, facility, cloud service, or security protection asset, the scope question should be escalated immediately. Scope cannot be managed by quietly excluding inconvenient systems.

Useful evidence for this topic includes scope issue log, updated diagram, data-flow evidence, provider record, decision documentation. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.36 Use Daily Closeout to Prevent Accumulated Confusion

Use Daily Closeout to Prevent Accumulated Confusion is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. At the end of each assessment day, Harbor Point should reconcile completed interviews, open evidence requests, pending demonstrations, scope issues, potential findings, provider dependencies, and the next day schedule. The internal closeout should not become a forum for inventing new answers.

Useful evidence for this topic includes daily closeout record, open-request list, schedule update, issue log, owner assignments. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.37 Keep Executive Communications Factual and Proportionate

Keep Executive Communications Factual and Proportionate is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Executives need a concise view of progress, material issues, unresolved dependencies, and decisions required. They do not need a minute-by-minute transcript. Overstating every assessor question as a failure creates unnecessary pressure and can drive bad decisions.

Useful evidence for this topic includes executive status note, material issue list, decisions required, schedule risk, remediation trigger. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.38 Manage Provider Dependencies in Real Time

Manage Provider Dependencies in Real Time is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A delayed cloud export, unavailable MSSP analyst, or inaccessible log archive can stall the assessment. Harbor Point should know which requests depend on NorthStar, Beacon, or another provider and escalate those dependencies before they become assessment-day surprises.

Useful evidence for this topic includes provider request queue, SLA, escalation path, provider owner, delivery timestamps. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.39 Harbor Point Scenario: Opening Meeting Reveals a Scope Mismatch

Harbor Point Scenario: Opening Meeting Reveals a Scope Mismatch is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. During the opening meeting, the assessor asks about a remote administration gateway that appears on a current network diagram but not in the assessment scope package. Harbor Point does not minimize the issue. NorthStar explains the gateway function, access model, and customer use, while the customer coordinator opens a formal scope issue for resolution.

Useful evidence for this topic includes current diagram, gateway configuration, remote-access records, scope package, decision log. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.40 Harbor Point Scenario: An Interview Answer Conflicts with the Procedure

Harbor Point Scenario: An Interview Answer Conflicts with the Procedure is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A Harbor Point manager says access reviews occur quarterly, while the procedure says monthly. The coordinator does not interrupt or correct the manager in real time. After the interview, Harbor Point retrieves the review history, determines the actual cadence, and provides a factual clarification supported by records.

Useful evidence for this topic includes procedure, access-review history, interview note, clarification record, corrective action if needed. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative

system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.41 Harbor Point Scenario: NorthStar Demonstrates Endpoint Enforcement

Harbor Point Scenario: NorthStar Demonstrates Endpoint Enforcement is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. The assessor asks to see endpoint security policy enforcement for Harbor Point laptops. NorthStar uses a Harbor Point tenant view, identifies the complete managed population, shows policy assignment and health status, and then opens one assessor-selected device record without exposing another customer.

Useful evidence for this topic includes tenant report, device population, policy assignment, selected device record, audit log. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.42 Harbor Point Scenario: Beacon Explains Alert Escalation

Harbor Point Scenario: Beacon Explains Alert Escalation is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Beacon demonstrates how a high-severity alert for Harbor Point is triaged, escalated, recorded, and handed to the customer. Harbor Point then explains who receives the escalation, who decides whether to invoke incident response, and how management notifications occur.

Useful evidence for this topic includes alert record, SOC case, escalation timestamp, customer ticket, incident procedure. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.43 Harbor Point Scenario: Evidence Is Missing

Harbor Point Scenario: Evidence Is Missing is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. The

assessor requests evidence of a recurring review for a prior period, and Harbor Point cannot locate it. The team states that the record is unavailable, searches approved repositories, provides related evidence only if it truly supports the objective, and opens corrective action rather than fabricating a missing review record.

Useful evidence for this topic includes repository search, related records, request tracker, gap record, corrective action ticket. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.44 Harbor Point Scenario: A Demonstration Fails

Harbor Point Scenario: A Demonstration Fails is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. A test account remains able to access a resource that the team expected to be blocked. NorthStar captures the result, stops further risky testing, preserves the configuration and logs, and opens a priority investigation. Harbor Point does not ask the assessor to ignore the outcome because the demonstration was unexpected.

Useful evidence for this topic includes test plan, failed result, logs, configuration snapshot, incident/change ticket. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.45 Harbor Point Scenario: A Provider Engineer Starts Answering for the Customer

Harbor Point Scenario: A Provider Engineer Starts Answering for the Customer is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. During an interview, a NorthStar engineer begins explaining Harbor Point management approval practices. The customer coordinator redirects the question to the Harbor Point owner and asks NorthStar to answer only the technical workflow it performs. This preserves both accuracy and responsibility boundaries.

Useful evidence for this topic includes responsibility matrix, interview roster, service description, customer approval records. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the

actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.46 Harbor Point Scenario: Daily Closeout Changes the Next Day

Harbor Point Scenario: Daily Closeout Changes the Next Day is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. At closeout, the team finds three evidence requests waiting on the same Beacon analyst and a technical demonstration dependent on a maintenance window. The coordinator re-sequences the next day, escalates the provider dependency, and informs the C3PAO of the logistical change without attempting to influence assessment conclusions.

Useful evidence for this topic includes daily closeout, updated schedule, provider escalation, request tracker, communication record. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.47 Translate Assessment Friction into MSP Service Improvement

Translate Assessment Friction into MSP Service Improvement is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. Every repeated evidence problem should become a service-design question. If customer-specific exports are difficult to retrieve, the MSP should improve reporting. If responsibility boundaries are unclear, update the service description and responsibility matrix. If demonstrations require unsafe access, redesign the support model.

Useful evidence for this topic includes lessons learned, service backlog, contract updates, runbook changes, evidence automation plan. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

18.48 Leave Assessment Week with a Stronger Operating Model

Leave Assessment Week with a Stronger Operating Model is an assessment-day discipline because the C3PAO must be able to evaluate the organization as it actually operates. The assessment should end with the environment more understandable than it was before. Harbor Point should know which records were difficult to retrieve, which roles were unclear, which provider dependencies created delay, and which controls were hard to demonstrate. Those lessons feed Chapter 19 and the remaining maturity work rather than disappearing when the assessors leave.

Useful evidence for this topic includes lessons-learned register, improvement plan, owners, due dates, validation schedule. These examples are practical methods rather than additional CMMC requirements. The evidence set should be tailored to the actual assessment request, the defined scope, and the authoritative system of record. A strong package identifies the customer, population or object, relevant time period, source, responsible owner, and relationship to the requirement being assessed.

Assessment-Day Field Guide for MSP-Supported Organizations

Assessment Stage	Operating Focus
Opening meeting	Confirm scope, participants, schedule, locations, evidence handling, communications, daily cadence, and known constraints.
Evidence requests	Record exact request, owner, source, time period, customer attribution, delivery status, and follow-up.
Interviews	Use actual responsible personnel. Prepare roles and evidence locations, not memorized scripts.
Demonstrations	Use customer-scoped views, controlled test objects, least privilege, logging, expected results, and cleanup.
Multi-tenant systems	Prevent exposure of other customers through filters, dedicated views, redaction, and controlled exports.
Missing or conflicting evidence	Preserve the truth, identify alternate authoritative evidence if it exists, and open corrective action rather than reconstructing history.
Potential findings	Capture facts, preserve original state, support factual corrections with records, and keep remediation separate from assessor independence.
Daily closeout	Reconcile open requests, scope issues, interviews, demonstrations, provider dependencies, potential

	findings, and next-day schedule.
End of assessment	Reconcile status, open actions, temporary access, retained evidence, lessons learned, and return to continuous readiness.

Implementation Checklist

- Confirm the authoritative assessment scope, SSP, network/data-flow diagrams, assets, ESPs, and provider responsibilities before the opening meeting.
- Name the customer assessment coordinator, backup coordinator, executive decision maker, technical lead, and provider points of contact.
- Publish one assessment calendar and identify interviews or demonstrations that depend on NorthStar, Beacon, cloud providers, or other third parties.
- Use one evidence-request tracker and preserve the original wording of each request.
- Confirm the approved evidence repository and secure transfer method; prohibit credentials and sensitive evidence in casual chat.
- Test that customer-specific exports can be produced from multi-tenant tools without exposing other customers.
- Prepare interviewees to explain their own responsibilities, normal workflow, exceptions, and evidence locations.
- Confirm executives understand governance, resources, risk decisions, accountability, and affirmation responsibilities applicable to their role.
- Prepare controlled demonstration plans for high-risk or privileged mechanisms.
- Use named, time-bounded privileged access during demonstrations and remove temporary access afterward.
- Identify the complete population before responding to a sample request when population context is relevant.
- Do not replace assessor-selected sample items with cleaner examples.
- Label test objects clearly so they cannot be confused with historical production records.
- Capture before-and-after state if remediation occurs during the assessment period.
- Escalate newly discovered scope issues immediately.
- Distinguish missing evidence from actual implementation failure using authoritative records.
- Use factual corrections only when a specific fact can be corrected with reliable evidence.

- Run a daily internal closeout without rewriting the story from that day.
- Provide executives with concise factual status, material issues, decisions required, and schedule risk.
- Track provider dependencies and escalate against contractual evidence/support expectations.
- Remove temporary assessment access after use and verify cleanup.
- Preserve lessons learned and convert repeated friction into service, contract, runbook, reporting, or training improvements.

Workshop 1 - Opening Meeting Simulation

Run a 45-minute opening meeting for Harbor Point. Reconcile scope, participants, locations, daily cadence, evidence transfer, communications, provider participation, and known constraints. Inject one scope mismatch and document how the team handles it.

Deliverable: create a reusable operating artifact that identifies owner, authoritative source, decision authority, evidence, and escalation path. The workshop is not complete when the discussion ends; it is complete when the improved operating method can be repeated by another qualified person.

Workshop 2 - Evidence Request Sprint

Issue twelve evidence requests over two hours. Require the team to assign owners, identify authoritative sources, produce customer-specific artifacts, record delivery, and capture follow-up. Measure response quality rather than only speed.

Workshop 3 - Interview Readiness Without Scripting

Assign five interview topics to customer, MSP, and MSSP personnel. Each person explains the real workflow in their own words, identifies evidence, and states where their responsibility ends. Review contradictions afterward.

Workshop 4 - Multi-Tenant Console Demonstration

Demonstrate endpoint or SIEM coverage for Harbor Point without showing another customer. Use a customer filter, assessor-selected object, named privileged account, activity logging, and cleanup.

Workshop 5 - Missing Evidence Drill

Remove one expected historical artifact from the exercise. Require the team to search approved sources, identify legitimate alternate evidence, state when evidence is unavailable, and open corrective action without reconstructing history.

Workshop 6 - Contradictory Evidence Drill

Provide an SSP statement that conflicts with a current configuration export. Require the team to determine the real state, preserve both records, explain the discrepancy, and decide whether a factual correction, scope update, or remediation action is appropriate.

Workshop 7 - Failed Technical Test

Create a demonstration that produces an unexpected result. Practice stopping safely, preserving the original state, notifying the customer owner, opening the correct operational record, and avoiding pressure to conceal the failure.

Workshop 8 - Provider Boundary Exercise

Give NorthStar a question about Harbor Point management approval and give Harbor Point a question about NorthStar console configuration. Practice redirecting each question to the responsible party without creating awkward gaps.

Workshop 9 - Daily Closeout

Using a simulated day of interviews, requests, and demos, create a closeout record containing completed work, open items, potential scope issues, provider dependencies, next-day schedule changes, and executive decisions required.

Workshop 10 - Assessment Friction to Service Improvement

Take ten problems observed during the simulation and turn each into a durable improvement: report automation, provider SLA, contract term, runbook change, role clarification, training, dashboard, repository change, or recurring validation task.

Practical Working Templates

Assessment-Day Contact and Escalation Record

Field	Record
Role	_____ _
Primary person	_____ _
Backup	_____ _
Organization	_____ _

Contact method	_____ _
Decision authority	_____ _
Escalation trigger	_____ _

Evidence Request Tracker

Field	Record
Request ID	_____ _
Date/time	_____ _
Exact request	_____ _
Assessment topic	_____ _
Customer owner	_____ _
Provider owner	_____ _
Authoritative source	_____ _
Scope/time period	_____ _
Delivered	_____ _
Follow-up	_____ _
Disposition	_____ _

Interview Schedule and Responsibility Record

Field	Record
Interview topic	_____ _

Primary interviewee	_____ _
Backup	_____ _
Customer/provider role	_____ _
Systems/processes covered	_____ _
Evidence location	_____ _
Schedule	_____ _
Notes	_____ _

Technical Demonstration Plan

Field	Record
Topic	_____ _
Purpose	_____ _
System/tenant	_____ _
Test object	_____ _
Operator	_____ _
Required privilege	_____ _
Expected behavior	_____ _
Evidence captured	_____ _
Rollback	_____ _
Cleanup	_____

	_

Scope Issue Record

Field	Record
Issue ID	_____ _
Discovered date/time	_____ _
System/service/data flow	_____ _
Why scope may be affected	_____ _
Immediate containment	_____ _
Owner	_____ _
C3PAO communication	_____ _
Decision	_____ _
Updated artifact	_____ _

Factual Correction Record

Field	Record
Issue ID	_____ _
Fact to correct	_____ _
Correct fact	_____ _
Authoritative evidence	_____ _
Submitted by/date	_____ _
C3PAO response	_____

	_
Disposition	_____ _

Daily Assessment Closeout

Field	Record
Date	_____ _
Completed interviews	_____ _
Completed demonstrations	_____ _
Requests closed	_____ _
Requests open	_____ _
Potential findings	_____ _
Scope issues	_____ _
Provider dependencies	_____ _
Next-day changes	_____ _
Executive decisions	_____ _

Assessment Lessons-Learned Record

Field	Record
Observed friction	_____ _
Root cause	_____ _
Customer impact	_____ _
Provider impact	_____

	_
Durable improvement	_____ _
Owner	_____ _
Due date	_____ _
Validation method	_____ _

Review Questions

1. Why should assessment day be treated as verification rather than performance?
2. What is the purpose of an assessment-day command structure?
3. What should be confirmed during the opening meeting?
4. Why must the assessment boundary be reconciled before evidence review?
5. Why do organizational and system identifiers matter during certification work?
6. What is the benefit of one authoritative assessment calendar?
7. Why should evidence not be transferred through casual chat?
8. What fields belong in an effective evidence request tracker?
9. How do examine, interview, and test differ?
10. Why can an assessment schedule change after the assessment begins?
11. What is the difference between preparing an interviewee and scripting an answer?
12. Why should an MSP not answer customer management questions?
13. What types of questions should executives be prepared to answer?
14. What should technical staff be able to demonstrate?
15. Why are service desk personnel useful interviewees?
16. What is the proper purpose of a follow-up interview?
17. Why should documentary evidence be presented in context?
18. What makes configuration evidence stronger than a product capability statement?
19. Why are logs and tickets valuable operational evidence?
20. What is the difference between point-in-time and sustained evidence?

21. Why should population coverage be understood before sampling?
22. Why should the organization not substitute cleaner sample items?
23. What belongs in a technical demonstration plan?
24. Why are controlled test objects useful?
25. What controls should surround privileged demonstrations?
26. How can an MSP protect other customers during a multi-tenant demonstration?
27. What special issues arise in a remote assessment?
28. What logistical controls may be necessary for an on-site assessment?
29. How should the team respond when requested evidence does not exist?
30. What should happen when the SSP conflicts with the real system state?
31. How does an evidence gap differ from an implementation gap?
32. What makes a factual correction credible?
33. How should the organization manage a potential finding?
34. Why must remediation preserve the original assessed state?
35. What should happen when a new scope issue is discovered?
36. What should be covered during daily closeout?
37. How should executives be briefed during assessment week?
38. Why should provider dependencies be tracked explicitly?
39. What does the Harbor Point failed-demonstration scenario teach?
40. How should assessment-day friction improve future MSP service delivery?

Answer Guidance

Questions 1 through 8 focus on opening governance, scope, communications, calendars, and request tracking. Strong answers emphasize one authoritative operating model, accurate scope, controlled evidence handling, and clear ownership.

Questions 9 through 16 focus on assessment methods and interviews. Strong answers distinguish examine, interview, and test; assign questions to the people who actually perform the work; and reject memorized or provider-authored customer answers.

Questions 17 through 28 focus on evidence, demonstrations, sampling, remote work, and multi-tenant protection. Strong answers make evidence customer-specific, contextual, historical where required, and safe to retrieve and demonstrate.

Questions 29 through 38 focus on missing or conflicting evidence, findings, scope changes, daily closeout, executives, and provider dependencies. Strong answers preserve facts, maintain assessor independence, and use controlled issue management rather than improvisation.

Questions 39 and 40 focus on the Harbor Point scenario and sustainment. Strong answers turn unexpected results and assessment friction into durable improvements in service design, reporting, contracts, runbooks, training, and continuous readiness.

Key Terms

Term	Working Meaning
Examine	Assessment method that evaluates documents, records, configurations, artifacts, and other evidence.
Interview	Assessment method that uses discussion with responsible personnel to understand how a process is performed and controlled.
Test	Assessment method that exercises or observes a mechanism, activity, or control behavior.
Population	The complete set of items relevant to an assessment question from which samples may be selected.
Sample	A subset of a defined population selected for detailed evaluation according to the applicable assessment approach.
Evidence Request Tracker	Operational record used to capture the exact request, owner, source, delivery, follow-up, and disposition.
Technical Demonstration	Controlled observation of a real mechanism or workflow to show how it behaves in the assessed environment.
Test Object	A dedicated account, file, device, alert, or other controlled object used to demonstrate behavior without unnecessary production risk.
Factual Correction	A narrow, evidence-supported correction of an inaccurate fact used or stated during assessment activity.
Scope Issue	A newly discovered fact that may change what systems, services, locations, data flows, providers, or assets belong in the assessment boundary.
Customer-Specific Evidence	Evidence clearly attributable to the assessed customer, tenant, system, population, or defined

	scope.
Multi-Tenant Safeguard	A method that enables provider evidence or demonstrations while preventing disclosure of unrelated customer information.
Daily Closeout	End-of-day reconciliation of assessment progress, open requests, issues, dependencies, and the next-day operating plan.
Assessment Coordinator	Customer role responsible for logistics, request routing, scheduling, and communications without controlling assessor conclusions.
Assessment Theater	Temporary or artificial behavior designed to appear compliant during assessment rather than represent normal operations.

Chapter Closing

Assessment day is where preparation becomes visible. A mature organization does not need to become someone different for the assessor. Its scope is understood, its personnel know what they actually do, its providers can explain their own responsibilities, its systems produce records through normal operations, and its evidence can be retrieved without reconstructing history. The assessment team is then able to evaluate a coherent operating environment rather than a temporary compliance performance.

For the MSP, the central discipline is controlled participation. NorthStar should make Harbor Point's managed environment easier to understand by producing customer-specific evidence, explaining technical services, supporting safe demonstrations, and being available when its personnel actually perform the function under review. Beacon should do the same for monitoring and security operations. Neither provider should answer for customer management, hide exceptions, expose other tenants, or confuse product capability with demonstrated implementation.

The most valuable assessment-day lesson is that friction is diagnostic. Slow evidence retrieval, contradictory answers, uncertain scope, unsafe demonstrations, provider delays, and undocumented exceptions all reveal where the operating model is weak. The organization should leave assessment week with a stronger service design, not merely a thicker evidence folder. That is how assessment experience becomes lasting readiness.

Official References

R1. Electronic Code of Federal Regulations. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Use the current provisions governing Level 2 certification assessments, assessment scope, status, POA&M treatment, affirmation, and related program requirements.

R2. U.S. Department of Defense Chief Information Officer. CMMC Assessment Guide - Level 2, Version 2.13. Provides assessment-method and evidence guidance for Level 2 self-assessments and certification assessments using the published CMMC Level 2 framework.

R3. U.S. Department of Defense Chief Information Officer. CMMC Resources & Documentation and About CMMC, reviewed September 20, 2026. DoD announced on July 13, 2026 that planned Phase II implementation was suspended while Phase I self-assessment requirements remain in place and the program undergoes review.

R4. Acquisition.gov. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025), and DFARS Subpart 204.75. Review the current contract clause and solicitation implementation applicable to the specific procurement.

R5. The Cyber AB. Current C3PAO authorization, assessment, assessor, impartiality, appeals, and certification-ecosystem resources applicable to an authorized C3PAO engagement.

R6. NIST SP 800-171 Revision 2 and NIST SP 800-171A (June 2018) as referenced by the published CMMC Level 2 assessment framework. Always follow the version incorporated by the governing CMMC rule and contract applicable to the engagement.

R7. Customer contracts, SSP, network and data-flow diagrams, service descriptions, responsibility matrices, provider agreements, evidence repositories, and current system records for the actual assessed environment.

Sources reviewed September 20, 2026. This chapter is educational and operational guidance. It does not replace 32 CFR Part 170, applicable FAR/DFARS clauses, current DoD CMMC implementation notices, authorized C3PAO procedures, the customer’s actual solicitation or contract, legal advice, or the independent determinations of the assessment team.

CMMC for MSPs: From Readiness to Certification

Chapter 19

After the Assessment

By Dr. Charles Edwards

Chapter 19 Contents

This Expanded Teaching Edition uses numbered headings throughout so the reader can navigate the chapter by topic. The emphasis is detailed explanation first, with checklists and tables used only after the underlying concept has been taught.

19.80-19.89 Common Mistakes and Institutional Knowledge
19.90-19.100 Readiness Checklists, Review, and Closing
19.101-19.205 Final Expansion Layer: Worked Examples and Operational Tools

Chapter Purpose

The assessment is over. For weeks - perhaps months - the defense contractor and its Managed Service Provider have prepared for this moment. Policies were reviewed, the System Security Plan was examined, evidence was organized, technicians verified configurations, employees participated in interviews, administrators demonstrated systems, and management responded to governance questions.

There may be an immediate feeling of relief. That reaction is understandable. But this is also one of the most dangerous moments in the CMMC lifecycle, because everyone wants to believe the work is finished.

> ***Can the organization continue operating this way tomorrow, next month, next year, and through the next assessment cycle?***

That is the subject of this chapter. We will examine the period after assessment from both sides of the relationship: the defense contractor that owns its contractual and organizational obligations, and the MSP that operates important portions of the technology and security environment.

19.1 The Assessment Is a Checkpoint, Not a Finish Line

One of the easiest mistakes to make with CMMC is to think of the assessment as the final destination. An organization spends months preparing, the assessment arrives, the assessment ends, everyone celebrates, and then the organization gradually returns to the way it operated before the assessment.

For a novice reader, the word assessment can make CMMC sound like a one-time examination. That is not the operating reality. An assessment examines whether required security practices are implemented at a point in time, but the people, systems, providers, and business processes being assessed continue to change immediately afterward. The organization therefore needs a way to preserve the security outcome while allowing normal business change to continue.

Harbor Point should not try to freeze its environment in the exact condition seen by an assessor. New employees will arrive, devices will be replaced, applications will change, and vulnerabilities will be discovered. The goal is controlled change: understand what is changing, determine whether security or scope is affected, make the change through an approved process, validate the result, and update the documentation and evidence when necessary.

CMMC readiness cannot be something an organization turns on shortly before an assessment and turns off afterward. The environment does not remain frozen simply because it was assessed. New employees arrive, laptops fail, firewall rules change, vulnerabilities appear, technicians leave, cloud applications are introduced, and business processes evolve.

19.2 Two Organizations Leave the Assessment

Harbor Point Engineering is our fictional defense contractor. NorthStar Managed Technology is Harbor Point's MSP. Beacon SOC provides security monitoring. When the assessment ends, all three organizations leave with responsibilities.

Harbor Point cannot say that NorthStar now handles CMMC. NorthStar cannot say the assessment belongs only to Harbor Point. Beacon cannot assume that sending alerts completes the entire incident-response process. The post-assessment environment remains a shared operating environment with clearly divided responsibilities.

19.3 Plain-English Translation: What Happens After an Assessment?

Think about a building that has just completed a fire-safety inspection. The inspector verifies alarms, exits, extinguishers, evacuation procedures, and emergency lighting. Passing the inspection does not eliminate the need for fire safety. The same principle applies to CMMC: the assessment evaluates implementation; it does not replace the security program.

Continuous readiness is easier to understand if we remove the compliance vocabulary. It means continuing to do tomorrow what the organization demonstrated yesterday. If access is supposed to be approved, it remains approved. If terminated users are supposed to lose access, the next terminated user also loses access. If backups are supposed to be recoverable, restoration continues to be tested after assessment week has passed.

This does not require employees to behave as though an assessor is permanently standing behind them. It requires dependable operations. When normal operations are dependable, assessment preparation becomes verification and organization rather than reconstruction.

19.4 What the Defense Contractor Should Be Thinking

The defense contractor should immediately ask what it learned. Were deficiencies identified? Which processes were difficult to demonstrate? Did documentation accurately describe reality? Were employees able to explain their responsibilities? Did responsibility boundaries become unclear? Did the assessment expose systems, providers, or information flows that management did not fully understand?

The defense contractor should use the end of the assessment as an opportunity to test its own understanding of the environment. Management should ask whether it can explain where relevant government information is handled, which systems and providers support that work, who has authority to make security decisions, and where responsibility is shared with an MSP or another service provider.

The contractor does not need to become its own MSP. It does, however, need enough understanding to govern the outsourced relationship. A company cannot make informed decisions about access, providers, risk, or contractual obligations if it does not understand the environment at a business level.

19.5 What the MSP Should Be Thinking

The MSP should perform a parallel review. Which services were examined? Which technicians participated? Could customer-specific evidence be produced efficiently? Were privileged-access records complete? Could the MSP demonstrate MFA, patching, backup, logging, endpoint security, and change history without exposing other customers? Did the responsibility matrix match what the MSP actually performs?

The MSP should perform a parallel review from the service-delivery perspective. Which parts of the customer environment does the MSP actually administer? Which technicians can reach those systems? Which records can be produced by customer rather than only across the MSP's entire platform? Which activities depend on another provider, such as a SOC or cloud service?

This review is valuable beyond assessment preparation. If the MSP cannot quickly determine who has privileged access to a customer, which endpoints are missing security agents, or whether backups were recently restored successfully, the assessment has exposed an operational weakness that deserves correction.

19.6 The First Post-Assessment Meeting

Hold a formal post-assessment meeting as soon as practical. Do not wait a month. Memories fade and small details disappear. The purpose is not to argue about the assessor; it is to learn while the experience is fresh.

The first post-assessment meeting should occur while the experience is still fresh. Participants should separate formal assessment results from internal lessons learned. A difficult evidence request may not have produced a formal finding, yet it can still reveal that the organization depends on manual searches, individual memory, or unclear responsibility.

The meeting should be factual rather than defensive. The useful question is not who looked bad during the assessment. The useful question is why the process was difficult and what change would make the next occurrence easier, safer, and more repeatable.

19.7 Findings Versus Lessons

Not every lesson from an assessment appears as a formal finding. An assessor may accept the evidence while the organization still discovers that producing it was unnecessarily difficult. That operational friction should be recorded and improved even when it does not become a formal deficiency.

19.8 Assessment Friction

Assessment friction is difficulty demonstrating something the organization believes it already does. Evidence may take hours to locate, reports may disagree, technicians may explain the same process differently, documentation may not match configuration, or customer/MSP responsibility may be unclear. Friction is valuable because it identifies where the operating model is fragile.

Assessment friction is the gap between doing something and being able to explain or demonstrate it reliably. A security capability may exist, but the supporting records may be scattered across several systems. Two technicians may perform the same task differently. The SSP may describe an older process. A customer may believe the MSP owns a responsibility that the MSP believes belongs to the customer.

Friction is valuable because it identifies fragility before that fragility becomes a larger failure. The organization should record the lesson even when no formal deficiency is issued.

19.9 The Post-Assessment Action Register

Create a Post-Assessment Action Register that is broader than a formal CMMC POA&M. It can track formal findings, documentation corrections, evidence improvements, operational weaknesses, training issues, automation opportunities, and responsibility problems.

The action register should be broader than a formal assessment POA&M. It is an internal management tool that captures what the organization learned and makes the lesson visible until it is resolved. Each item should identify the problem in plain language, the responsible owner, supporting parties, target date, validation method, evidence expected, and any documentation that may need to change.

For example, “privileged access report difficult to generate” is more useful when expanded to explain that NorthStar had to search its RMM, cloud roles, firewall portal, backup console, password vault, and customer-specific accounts before it could identify everyone with Harbor Point administrative access. That description points toward a real process improvement rather than a cosmetic report.

ID	Issue	Owner	Priority	Target	Evidence of Completion
PA-001	Privileged access report difficult to generate	NorthStar	High	30 days	Automated customer report
PA-002	Network diagram missing new segment	Harbor Point	High	10 days	Approved revised diagram
PA-003	SIEM escalation workflow unclear	Beacon/ NorthStar	High	20 days	Updated workflow and test
PA-004	Backup restore evidence inconsistent	NorthStar	Medium	30 days	Completed restore test
PA-005	Employee unsure how to report suspicious email	Harbor Point	Medium	15 days	Training record

19.10 Understanding the Word Remediation

In plain English, remediation means correcting a problem. Strong remediation goes further than fixing the visible symptom: it asks why the problem happened and changes the process so the same weakness is less likely to recur.

19.11 Root Cause Matters

If former MSP technicians still have access, removing their access is necessary but incomplete. The organization should determine why offboarding failed, whether other accounts are affected, and whether the access-review process should have detected the problem earlier.

Root-cause analysis asks why the problem was able to exist. If two former technicians still have customer-specific accounts, disabling those accounts is necessary, but the organization should also ask why the offboarding workflow did not remove them. Perhaps the accounts were outside centralized identity management. Perhaps the customer-specific access register was incomplete. Perhaps nobody was assigned to verify removal.

The objective is not to create an elaborate investigation for every minor issue. It is to avoid repeatedly correcting the same symptom while leaving the underlying process unchanged.

19.12 Symptom Correction Versus Root-Cause Correction

Removing three stale accounts is symptom correction. Fixing the offboarding workflow, reviewing similar accounts, updating the privileged-access inventory, testing the corrected process, and preserving evidence is root-cause correction.

19.13 Root-Cause Worksheet

A useful worksheet captures the problem, immediate risk, immediate correction, why it happened, why it was not detected, the underlying process failure, corrective action, validation method, and evidence.

19.14 Introducing the CMMC POA&M

POA&M stands for Plan of Action and Milestones. In ordinary language, it is a formal plan for correcting certain security deficiencies when the CMMC framework

permits those deficiencies to be placed on such a plan. It is not permission to postpone any control the organization does not feel like completing.

POA&M means Plan of Action and Milestones. A novice reader should resist the temptation to use the acronym as a synonym for any unfinished cybersecurity work. In the CMMC assessment context, a formal assessment POA&M is governed by specific eligibility, scoring, and closeout rules. Ordinary maintenance tasks, future improvements, and operational exceptions are not automatically CMMC assessment POA&Ms.

The practical lesson is to label work accurately. A vulnerability discovered during normal operations may need an operational plan and documented remediation, but that does not mean the organization should retroactively treat the matter as though it were an assessment POA&M.

19.15 Why a POA&M Is Not an Ordinary To-Do List

Routine technology improvements and operational tasks may belong in normal planning. A CMMC POA&M belongs to the formal assessment context and is governed by specific rules. Organizations should not call every cybersecurity task a POA&M.

POA&M means Plan of Action and Milestones. A novice reader should resist the temptation to use the acronym as a synonym for any unfinished cybersecurity work. In the CMMC assessment context, a formal assessment POA&M is governed by specific eligibility, scoring, and closeout rules. Ordinary maintenance tasks, future improvements, and operational exceptions are not automatically CMMC assessment POA&Ms.

The practical lesson is to label work accurately. A vulnerability discovered during normal operations may need an operational plan and documented remediation, but that does not mean the organization should retroactively treat the matter as though it were an assessment POA&M.

19.16 Operational Plans of Action

An operational plan of action can be used to manage vulnerabilities, temporary deficiencies, patches, maintenance issues, and other operational problems arising after implementation. The concept should not be confused with a formal assessment POA&M.

19.17 The 180-Day Window

Where current Level 2 rules permit a conditional result with an assessment POA&M, applicable closeout must occur within the required 180-day period. Six months can disappear quickly when remediation requires analysis, procurement, deployment, testing, documentation, training, evidence collection, and closeout.

Six months sounds generous until the organization maps the actual work. A corrective action may require root-cause analysis, design, management approval, procurement, implementation, testing, user coordination, documentation updates, evidence collection, and applicable closeout activity. If another provider or software vendor is involved, scheduling delays can consume additional time.

That is why qualifying assessment remediation should begin immediately. Day One should establish ownership, milestones, dependencies, validation, evidence, and management visibility rather than merely placing the item in a general help-desk queue.

19.18 Day One Means Day One

Treat the first business day after assessment as Day One of remediation. Assign an owner, technical lead, customer responsibility, MSP responsibility, external-provider dependency, target date, validation method, evidence requirement, and documentation impact.

19.19 Customer/MSP Remediation Matrix

Activity	**Harbor Point**	**NorthStar**	**Beacon**
Approve corrective action	Accountable	Consulted	Consulted
Modify endpoint configuration	Consulted	Responsible	-
Validate SIEM ingestion	Consulted	Consulted	Responsible
Update SSP	Responsible	Consulted	Consulted
Produce technical evidence	Consulted	Responsible	Responsible
Validate business impact	Responsible	Consulted	-
Approve closure	Responsible	Consulted	Consulted

19.20 A Practical Remediation Story

A shared-service finding should be followed from problem definition through responsibility assignment, corrective action, testing, evidence, and operationalization. For example, if Beacon generates alerts correctly but escalation between Beacon, NorthStar, and Harbor Point is inconsistent, the answer is not merely to rewrite a policy. The actual handoff must be mapped, tested, and documented.

19.21 Evidence of Remediation

A strong remediation evidence package explains the original issue, root cause, corrective action, implementation record, validation method, updated documentation, and supporting records. The package should allow another qualified person to understand what changed and why.

19.22 Evidence Should Tell a Story

Evidence should have context. A screenshot showing MFA enabled may be useful, but the reviewer also needs to understand whose account it represents, which tenant, when it was captured, whether it shows configuration or enforcement, and whether the sample represents the relevant population.

19.23 Closeout

Closeout is the applicable process for verifying that qualifying deficiencies have been corrected. The key beginner lesson is simple: the organization does not merely say that it fixed the issue; the applicable closeout process verifies the correction.

19.24 What Happens If Closeout Fails?

A formal assessment POA&M should be treated as an executive-level issue because failure to complete applicable closeout within the required period can affect conditional status. It should not disappear into an ordinary help-desk queue.

19.25 From Remediation to Continuous Readiness

After immediate findings are resolved, the organization transitions to continuous readiness: maintaining the security program and its supporting evidence through normal operations.

Continuous readiness is not continuous panic. It is the opposite. The purpose of integrating security into normal operations is to reduce the need for emergency preparation. When asset inventories are maintained, access reviews occur on schedule, change records are meaningful, backups are tested, and documentation is updated as the environment changes, the organization is less dependent on last-minute cleanup.

A useful test is whether an unexpected request for evidence would require days of reconstruction or whether the organization could retrieve dependable operational records from the systems it already uses.

19.26 What Continuous Readiness Looks Like

Continuous readiness means knowing the current scope, where FCI and CUI reside, who has administrative access, what changed, what vulnerabilities remain open, whether backups work, whether security logs are collected, what incidents occurred, and whether documentation still reflects reality.

19.27 The Difference Between Continuous Readiness and Continuous Panic

Continuous readiness does not mean spending every day preparing for an assessor. It means designing operations so that secure behavior and useful records happen naturally.

19.28 Evidence as a Byproduct of Good Operations

The strongest evidence is often a byproduct of good operations. Quarterly access reviews, approved change tickets, restore-test records, offboarding tickets, vulnerability reports, and incident records exist because the organization is operating securely, not because someone rushed to create screenshots before an assessment.

The strongest evidence usually begins as an operational record. An approved access request exists because someone needed access. A change ticket exists because a configuration changed. A restore-test record exists because the organization needed to know that recovery works. A vulnerability ticket exists because a weakness needed remediation.

When these records are complete and understandable, they can also demonstrate that the security process operates over time. This is more sustainable than creating special screenshots and spreadsheets only when an assessment approaches.

19.29 The MSP's Role After the Assessment

After assessment, the MSP's mindset changes from helping the customer get ready to helping the customer stay ready. Customer-specific security requirements, evidence, access, change control, vulnerability remediation, logging, backup, incident handling, and documentation become part of service delivery.

19.30 What the Contractor Cannot Outsource

A defense contractor can outsource many technical functions, but it cannot outsource understanding of its contracts, information, business processes, approvals, personnel, and governance. An MSP can operate technology; it cannot replace customer governance.

19.31 What the MSP Cannot Ignore

An MSP cannot ignore CMMC simply because the customer holds the defense contract. If the MSP administers systems, manages identities, stores backups, operates security tools, or generates logs, its operations may directly affect the customer's ability to demonstrate security requirements.

19.32 The Shared-Responsibility Conversation

Customer and MSP should be able to answer who creates accounts, approves access, reviews privileges, deploys patches, approves exceptions, monitors alerts, responds after hours, manages backups, updates documentation, and retains evidence. Shared responsibility must not become shared ambiguity.

Shared responsibility should be broken into specific actions. For identity management, Harbor Point may approve access, NorthStar may create the account and enforce MFA, and Harbor Point may notify NorthStar when employment ends. For incident response, Beacon may detect an event, NorthStar may perform technical containment, and Harbor Point may make business and contractual decisions.

The phrase shared responsibility becomes useful only when each handoff is understood. Otherwise, it can become a polite way of saying that nobody is certain who is supposed to act.

19.33 Configuration Drift

Configuration drift is the gradual movement of systems away from their intended or documented security state. Temporary firewall rules, stale admin accounts, missing logging agents, unhealthy endpoints, and MFA exceptions can accumulate even when nobody intends to weaken security.

Configuration drift is the gradual movement away from the intended security state. It usually occurs through ordinary work rather than deliberate neglect. A temporary firewall rule is never removed. An administrator receives elevated access for a project and keeps it afterward. A replacement server is deployed without the expected logging agent. An endpoint security service fails while the user continues working.

The defense against drift is not a prohibition on change. It is a disciplined process that detects exceptions, validates important configurations, reviews temporary access, monitors security-agent health, and connects significant changes to documentation updates.

19.34 Why Drift Happens

Drift usually grows out of ordinary operational pressure: emergency access, troubleshooting, urgent deployments, temporary exceptions, and restored systems. The problem occurs when temporary changes become permanent.

19.35 The CMMC Impact Question

Add a simple question to significant change workflows: Could this change affect CMMC scope, a security requirement, CUI handling, evidence, or documented architecture? That question can trigger deeper review where appropriate.

19.36 Shadow IT

Shadow IT occurs when departments or employees introduce technology outside normal IT and security processes. A convenient cloud service can become a governance problem if CUI is uploaded, the MSP is unaware, and the SSP is never updated.

Shadow IT occurs when technology is introduced outside the normal technology and security process. A business unit may purchase a useful cloud service with a credit card and begin using it before the MSP or security coordinator knows it exists. If FCI

or CUI later flows through that service, the organization can create an unmanaged part of its environment without intending to do so.

The solution is not to make technology adoption impossible. Employees should know when a new application, external sharing workflow, subcontractor connection, or cloud service needs review before sensitive information is placed into it.

19.37 When the MSP Changes Its Own Technology

When an MSP changes its own RMM, backup, security, or identity platforms, it should consider whether the change affects customer administrative access, authentication, logging, evidence, isolation, or documented architecture.

19.38 Personnel Changes

Personnel changes can alter security just as technology changes do. A dependable lifecycle is Personnel Event -> Authorization Decision -> Access Change -> Verification -> Evidence.

Personnel events are security events because access follows people. Hiring, termination, promotion, transfer, leave, contractor expiration, and MSP technician reassignment can all change what access is appropriate. The business event should trigger an access decision, the technical systems should implement that decision, and someone should verify the result.

For MSPs, this can be especially complicated because a technician may have corporate access plus customer-specific access in firewalls, cloud tenants, password vaults, backup systems, security consoles, and emergency accounts. A reliable offboarding process has to account for those separate access paths.

19.39 MSP Technician Offboarding

MSP technician offboarding must include corporate identity, VPN, RMM, PSA, password vault, EDR, backup, SIEM, firewall portals, cloud roles, and customer-specific accounts where applicable.

19.40 Offboarding Evidence

Offboarding evidence may include the HR trigger, ticket, account disablement, role removal, vault removal, VPN removal, customer-specific access removal, and manager verification.

19.41 Onboarding a New Technician

A newly hired MSP engineer should not automatically receive every customer's administrative access. Customer access should be based on business need, role, approval, training, least privilege, MFA, recording, and periodic review.

19.42 Customer Personnel Changes

Customer employees also change roles. An engineer who moves from a defense program to a commercial program may no longer need CUI access even though the person remains employed.

Personnel events are security events because access follows people. Hiring, termination, promotion, transfer, leave, contractor expiration, and MSP technician reassignment can all change what access is appropriate. The business event should trigger an access decision, the technical systems should implement that decision, and someone should verify the result.

For MSPs, this can be especially complicated because a technician may have corporate access plus customer-specific access in firewalls, cloud tenants, password vaults, backup systems, security consoles, and emergency accounts. A reliable offboarding process has to account for those separate access paths.

19.43 Vulnerability Management Never Ends

Vulnerability management continues after assessment: discover, analyze, prioritize, remediate, validate, and document. The MSP may perform much of the technical work, but the contractor still needs visibility into significant risk.

Vulnerability management is a cycle rather than a monthly patch event. The organization discovers weaknesses, evaluates their significance, prioritizes them, remediates them, validates the result, and documents important exceptions. A patching schedule is one part of that cycle, not the entire program.

When a patch cannot be installed immediately, the organization should understand why, assess the risk, consider temporary protections, identify the responsible owner, and establish a path to final remediation. Silence is not an exception process.

19.44 The Vulnerability Exception Problem

When a critical patch cannot be installed because it breaks a production application, the organization should document the reason, risk, temporary protection, approval, review date, and path to remediation rather than silently ignoring the vulnerability.

19.45 Patch Management After Assessment

Patch management requires inventory, prioritization, testing, deployment, exception handling, verification, and reporting. For MSPs, customer-specific reporting is particularly important.

19.46 Logging and Monitoring

Logging can degrade quietly when new systems are introduced without the required agents or configuration. New-system onboarding should trigger logging and monitoring checks.

Logging is useful only when the expected systems actually produce the expected telemetry and someone can act on meaningful events. A newly deployed server can be fully functional for users while still being invisible to the SOC if the logging agent was omitted or misconfigured.

New-system onboarding should therefore verify monitoring as an end-to-end outcome: the agent is installed, the platform receives events, the correct policy applies, and the escalation path is known.

19.47 Beacon SOC After the Assessment

Beacon's post-assessment work includes collecting telemetry, investigating alerts, escalating according to defined procedures, retaining records, and periodically validating the handoff with NorthStar and Harbor Point.

19.48 Backup and Recovery

A successful backup report is not the same as successful recovery. Mature operations test restoration, document what was restored, validate the result, and preserve the test record.

A successful backup job is encouraging, but it is not the same as proven recoverability. Recovery testing asks whether the organization can actually restore the needed data or system and verify that the restored result is usable.

NorthStar may perform the technical restore, while Harbor Point identifies which systems and data are most important to the business. The resulting test record should explain what was restored, from which backup, when the test occurred, who performed it, whether validation succeeded, and what corrective action was needed.

19.49 Incident Response After Assessment

An actual incident may test the program more severely than an assessment. Roles for detection, containment, customer notification, evidence preservation, business decisions, and contractual reporting should be understood before an incident occurs.

Incident response is a chain of decisions and handoffs. Beacon may detect suspicious activity, NorthStar may investigate and contain the technical problem, and Harbor Point may decide how the incident affects business operations and contractual obligations. A written plan is useful only if those handoffs work in practice.

Tabletop exercises allow the organizations to test the chain without waiting for a real emergency. A realistic scenario can reveal unclear contact paths, approval delays, missing after-hours coverage, and uncertainty about who preserves evidence or communicates with management.

19.50 Incident Response Tabletop Exercises

Tabletop exercises walk through a hypothetical incident and reveal unclear handoffs without requiring a real breach. They test who notices, who acts, who approves, who communicates, and what records are produced.

Incident response is a chain of decisions and handoffs. Beacon may detect suspicious activity, NorthStar may investigate and contain the technical problem, and Harbor Point may decide how the incident affects business operations and contractual obligations. A written plan is useful only if those handoffs work in practice.

Tabletop exercises allow the organizations to test the chain without waiting for a real emergency. A realistic scenario can reveal unclear contact paths, approval delays, missing after-hours coverage, and uncertainty about who preserves evidence or communicates with management.

19.51 Keeping the SSP Current

The System Security Plan should evolve when systems, locations, providers, security tools, network architecture, CUI flows, or responsibility boundaries materially change.

The System Security Plan is a description of implementation, not a security control by itself. Writing that MFA is enforced does not make MFA function. Conversely, a well-configured environment can still create assessment difficulty if the SSP describes an obsolete architecture or responsibility model.

The practical goal is alignment between documentation and reality. Significant changes to systems, providers, CUI flows, network architecture, administrative models, or security tools should trigger an appropriate documentation review.

19.52 The SSP Is Not the Environment

The SSP does not make the environment secure. It describes implementation. Strong readiness requires alignment between documentation and reality.

The System Security Plan is a description of implementation, not a security control by itself. Writing that MFA is enforced does not make MFA function. Conversely, a well-configured environment can still create assessment difficulty if the SSP describes an obsolete architecture or responsibility model.

The practical goal is alignment between documentation and reality. Significant changes to systems, providers, CUI flows, network architecture, administrative models, or security tools should trigger an appropriate documentation review.

19.53 Updating the Responsibility Matrix

Responsibility matrices must evolve when providers or services change. If scanning, backup, monitoring, or identity administration moves to another provider, ownership, evidence, and handoffs should be updated.

19.54 Changing MSPs

Changing MSPs affects administrative access, configuration records, backups, asset inventories, diagrams, ticket history, evidence, and customer-specific procedures. The transition must be controlled.

Changing MSPs is both a business transition and a security transition. The outgoing MSP may hold administrative access, configuration knowledge, historical tickets, backup responsibilities, vulnerability records, asset information, and evidence that the contractor may later need.

A controlled transition identifies what the outgoing MSP performs, transfers necessary knowledge and records, establishes the incoming MSP's access, validates continuity of monitoring and backup, removes the outgoing MSP's access at the correct time, and updates the SSP and responsibility matrix where necessary.

19.55 MSP Transition Checklist

An MSP transition should address responsibility transfer, access transfer and revocation, documentation, evidence, logging, backup custody, security-tool changes, SSP updates, responsibility-matrix updates, and validation.

19.56 Evidence Retention

Evidence retention should be based on applicable contractual, assessment, cybersecurity, legal, and business needs. Evidence may itself be sensitive and should be protected accordingly.

Evidence retention should be deliberate rather than unlimited. Security evidence may contain network diagrams, administrator names, vulnerability details, incident information, screenshots, configuration information, or CUI. The repository therefore deserves access control, monitoring, backup, and secure disposal practices appropriate to the information it contains.

The organization should retain records according to applicable contractual, legal, policy, operational, and assessment needs. The objective is to preserve what is needed without creating an uncontrolled archive of sensitive information.

19.57 The Ticketing System as an Evidence Engine

An MSP's PSA or ticketing system can become a powerful evidence source if tickets identify the customer, asset, issue, action, validation, and time. 'Fixed issue. Closed.' is rarely enough context.

19.58 Evidence Automation

Automated asset, endpoint, encryption, patch, vulnerability, access, backup, and alert reports can reduce manual effort. Automation does not eliminate the need for context and review.

19.59 Continuous Monitoring Does Not Mean Watching Everything Every Second

Continuous monitoring does not necessarily mean a human watches every system every second. Different activities can be reviewed daily, weekly, monthly, quarterly, or annually according to risk and applicable requirements.

19.60 The CMMC Operations Dashboard

An operational dashboard can show managed endpoints, encryption coverage, overdue vulnerabilities, MFA exceptions, backup failures, open remediation, and documentation status. It should not pretend to calculate a simplistic compliance percentage.

19.61 Annual Affirmation

Affirmation is a formal attestation by an authorized organizational official regarding the organization's CMMC status as required by the program. It should not be treated as a meaningless administrative click.

Affirmation should be treated as a governance activity. Management does not need to inspect every technical setting, but the authorized official should receive enough current information to understand the organization's scope, major changes, significant open issues, provider changes, privileged-access status, documentation accuracy, and security operations.

An affirmation process that consists only of sending an executive a link and saying “click here” misses the purpose of informed organizational responsibility.

19.62 Preparing Management to Affirm

Before management affirms, it should receive enough information to understand scope, major changes, access, vulnerabilities, incidents, provider changes, documentation status, and open remediation.

19.63 Level 1: The Small Defense Contractor

Pine Valley Precision Components is a 22-person fictional manufacturer used to illustrate the needs of a small Level 1 defense contractor that relies heavily on an MSP.

A small Level 1 contractor does not need to imitate the bureaucracy of a large enterprise. It does need to understand which systems and people are involved, what its MSP performs, what remains the contractor's responsibility, and whether the required safeguards continue to operate throughout the year.

Pine Valley demonstrates that the customer can remain accountable without becoming a security engineering company. The owner communicates business events and approves access; the MSP performs much of the technical implementation; both review significant changes and maintain enough records to understand the environment.

19.64 What Pine Valley Needs to Understand

Pine Valley's owner does not need to become a security engineer. The owner does need to understand why CMMC applies, what FCI is, which systems are involved, what the MSP does, what Pine Valley still owns, how the annual self-assessment works, and what evidence should exist.

19.65 Level 1 Is Not No Security

Level 1 should not be mistaken for 'no security.' Basic safeguarding requirements must actually be implemented, and current CMMC rules do not permit Level 1 assessment POA&Ms.

19.66 Pine Valley and Its MSP

If Pine Valley's MSP manages accounts, endpoints, firewall, backup, and Microsoft 365, Pine Valley still decides who should have access, communicates terminations, identifies relevant contracts and information, and governs business behavior.

19.67 Level 1 Annual Readiness Cycle

A small Level 1 contractor can maintain readiness through monthly security discussions, quarterly access and asset reviews, review of significant technology

changes, annual safeguard verification, self-assessment, affirmation, and continued operation.

19.68 Level 2: Harbor Point's Continuing Program

Harbor Point's Level 2 environment spans personnel, NorthStar, Beacon, cloud services, endpoints, networks, identity systems, and security platforms. The operational lesson is that a multi-year assessment cycle does not mean multi-year gaps between security reviews.

A Level 2 environment may include many more systems, providers, identities, security tools, and CUI workflows. The multi-year assessment cycle can create a false sense that there is plenty of time before readiness matters again. In reality, three years is enough time for the environment to change dramatically.

Harbor Point therefore uses recurring reviews to keep scope, access, providers, vulnerabilities, monitoring, backup, incident response, documentation, and evidence aligned between assessment events.

19.69 The Three-Year Trap

Three years is enough time for extensive personnel, technology, provider, and business change. The next assessment should not be the first time those changes are examined.

19.70 The 30-Day Post-Assessment Plan

During the first 30 days, conduct lessons learned, assign remediation, correct urgent problems, update inaccurate documentation, review responsibility boundaries and privileged access, verify inventory, and establish the continuous-readiness schedule.

The first 30 days are about understanding and stabilization. The organization captures lessons while they are fresh, assigns remediation, corrects urgent weaknesses, verifies privileged access and asset information, and identifies documentation that no longer matches reality.

The key is to understand why each action matters. Reviewing privileged access means identifying the people and accounts with elevated authority across cloud, firewall, RMM, backup, security, and customer-specific systems, then confirming that each access path is still required and appropriately approved.

19.71 The 60-Day Plan

By approximately Day 60, significant remediation should be progressing, evidence improvements underway, ticket templates refined, recurring reporting available, access reviews validated, and documentation aligned with corrections.

During the next period, corrections should become repeatable processes. A one-time privileged-access spreadsheet is not enough if it will be obsolete next month. The register should connect to technician onboarding, reassignment, offboarding, and recurring review. The same principle applies to restore testing, incident escalation, documentation updates, and evidence collection.

This is where the organization moves from “we fixed the issue” to “we changed the process that produces the outcome.”

19.72 The 90-Day Plan

By approximately Day 90, lessons should have become process improvements, recurring reviews should be operating, evidence should be generated naturally, roles should be understood, and management should have visibility.

By approximately Day 90, the organization should test the new operating model. Ask for the current privileged-access report and sample it against source systems. Trace a recent termination from business notification through access removal. Review a recent significant change and verify that documentation impact was considered. Perform a restore test and an incident tabletop.

The objective is not another mini-assessment. It is practical validation that the improvements are working during ordinary operations.

19.73 What Management Should Review Quarterly

Quarterly management review should consider scope changes, new systems and providers, CUI-flow changes, critical vulnerabilities, privileged access, incidents, backup, remediation, and SSP accuracy.

19.74 What the MSP Should Review Monthly

Monthly MSP reviews can cover endpoint health, patch status, vulnerabilities, backup, alerts, access changes, assets, configuration exceptions, open security tickets, and significant changes.

19.75 What the Defense Contractor Should Expect From Its MSP

A defense contractor should expect clear service descriptions, controlled administrative access, customer-specific records, meaningful change history, incident coordination, timely offboarding, technical evidence, assessment cooperation, and communication about material service changes.

A defense contractor should expect its MSP to understand and consistently perform the services assigned to it. That includes controlling technician access, documenting significant changes, maintaining customer-specific operational records, communicating material service changes, supporting incident response, and producing appropriate technical evidence for the functions it performs.

The expectation should be precise. “Make us compliant” is not a useful service description. “Manage endpoint security, patching, backup, and privileged MSP access according to the agreed procedures and provide customer-specific operational records” is much clearer.

19.76 What the MSP Needs From the Defense Contractor

The MSP needs the contractor to communicate new contracts, CUI workflows, locations, employees, terminations, subcontractors, applications, acquisitions, incidents, and requirement changes. An MSP cannot protect an environment it does not know exists.

The MSP needs timely business information from the customer. New contracts, locations, employees, terminations, subcontractors, applications, CUI workflows, acquisitions, and major process changes can all affect the environment the MSP is expected to protect.

This is why the sentence “nobody told IT” is so dangerous. An MSP cannot reliably secure a system, workflow, or provider relationship that the customer introduced without communication.

19.77 The Dangerous Sentence: Nobody Told IT

Many failures begin with 'Nobody told IT.' Continuous readiness requires organizational communication, not merely security software.

19.78 Harbor Point One Year Later

One year later, Harbor Point has changed: employees have joined and left, tools have changed, systems have been replaced, and a new subcontractor has appeared. The question is not whether the organization changed, but whether it changed under control.

One year after assessment, a healthy environment will not look identical to assessment day. People have joined and left, devices have been replaced, vulnerabilities have been remediated, tools have changed, and new business needs have appeared. The question is whether those changes were controlled and whether the security program remained aligned with reality.

This is the strongest sign that CMMC has moved from a temporary project into an operating discipline: the organization can explain how it changed, why it changed, who approved important changes, and how security and documentation were maintained through the change.

19.79 The One-Year Review

The one-year review confirms that inventory, access, security controls, documentation, provider relationships, and evidence remain aligned with the current environment.

19.80-19.89 Common Mistakes and Institutional Knowledge

Declaring victory after the assessment instead of maintaining the program. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Keeping the temporary assessment team separate from daily operations. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Freezing the SSP and diagrams while the environment continues to change. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that

prevents the problem from recurring and assign clear ownership for maintaining that process.

Assuming the MSP will notice business or technology changes it was never told about. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Assuming the customer understands material changes to MSP platforms without communication. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Treating evidence as a separate last-minute job rather than an operational byproduct. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Collecting too much evidence without context, ownership, or relevance. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Allowing one individual to become the only person who understands the CMMC environment. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Failing the 'bus test': if the primary coordinator or engineer disappears, the program cannot continue. This mistake is important because it separates assessment preparation from sustainable operations. The organization should identify the business or technical process that prevents the problem from recurring and assign clear ownership for maintaining that process.

Institutional knowledge should be strengthened through runbooks, responsibility matrices, architecture diagrams, standard operating procedures, ticket history,

customer profiles, and cross-training. The objective is not to eliminate expertise; it is to prevent the program from depending entirely on one person's memory.

19.90-19.100 Readiness Checklists, Review, and Closing

Post-Assessment Readiness Checklist

- Conduct lessons learned and record both formal issues and assessment friction.
- Assign remediation owners and target dates.
- Preserve evidence and update inaccurate documentation.
- Review asset inventory, CUI flow, privileged access, providers, and responsibility boundaries.
- Establish recurring management and MSP security reviews.
- Prepare management for applicable affirmation with current operational information.

Management Questions

182. Has our environment changed?
183. Has our scope changed?
184. Has our CUI flow changed?
185. Have our providers changed?
186. Have privileged users changed?
187. Are critical vulnerabilities controlled?
188. Are backups functioning?
189. Are security incidents being handled?
190. Does our documentation remain accurate?
191. Can we still demonstrate what we say we do?

> ***The ultimate continuous-readiness test is whether an earlier-than-expected assessment would create organizational panic or merely require logistics.***

Final Expansion Layer: From Assessment Results to Continuous Readiness

Continuous readiness is not continuous panic. It is the opposite. The purpose of integrating security into normal operations is to reduce the need for emergency preparation. When asset inventories are maintained, access reviews occur on schedule, change records are meaningful, backups are tested, and documentation is updated as the environment changes, the organization is less dependent on last-minute cleanup.

19.101 Why We Need to Go One Level Deeper

Understanding a concept is not the same as being able to implement it. A contractor may know that findings require remediation but still need to know who owns the work, how root cause is determined, what evidence proves completion, and how the corrected process becomes part of normal operations. The following worked examples turn the chapter's principles into repeatable practice.

19.102-19.106 Harbor Point's First Post-Assessment Week

At 4:17 p.m. on Friday, Harbor Point's final assessment meeting ends. On Monday morning, Harbor Point, NorthStar, and Beacon meet for a lessons-learned review. The security coordinator sets the tone: the meeting is not about blame; it is about learning while the experience is fresh.

Category	Example
Formal assessment issues	Items communicated through the applicable assessment process
Evidence problems	Information existed but was difficult to retrieve or explain
Process problems	Actual workflows were inconsistent or fragile
Improvement opportunities	No formal finding, but the assessment revealed a better way to operate

The team converts those observations into a Post-Assessment Action Register. Every issue receives an identifiable owner or role, supporting parties, a target, and a validation method. 'IT' or 'the MSP' is too vague for important remediation; ownership must be operationally meaningful.

19.108-19.116 Worked Example: Privileged Access Reporting

NorthStar could identify its privileged Harbor Point technicians, but the information was fragmented across RMM, Microsoft administrative roles, firewall portals, the password vault, backup, EDR, SIEM, and customer-specific accounts. The root cause was not a slow engineer. The root cause was the absence of a centralized customer-specific view of privileged access.

192. Define the problem precisely.
193. Determine the security impact.
194. Identify the root cause.
195. Design the corrective action.
196. Inventory and reconcile every relevant access path.
197. Remove unnecessary access.
198. Generate a customer-specific privileged-access report.
199. Sample the report against source systems to validate accuracy.
200. Preserve the remediation evidence.
201. Integrate the register into onboarding, offboarding, and recurring access review.

19.117-19.120 Worked Example: Incident Escalation

Beacon detects suspicious activity, NorthStar understands the customer systems, and Harbor Point owns business and contractual decisions. If the written procedure does not match the real handoff, the organizations must map and test the workflow rather than merely rewrite a paragraph.

Severity	Beacon	NorthStar	Harbor Point
Low	Record and monitor	Review in normal operations	No immediate action
Medium	Investigate and notify	Validate and remediate	Review as needed
High	Immediate escalation	Immediate technical response	Security coordinator notified
Critical	Immediate multi-party escalation	Containment support	Executive/incident process activated

The team then performs a tabletop exercise using suspicious privileged authentication followed by unusual file activity. The exercise records who was contacted, how, when, what decisions were required, and what evidence was produced.

19.121-19.124 Worked Examples: Documentation and Recovery

A missing network segment on the diagram is not merely a drawing problem if the change ticket existed but the documentation was never updated. The change workflow should ask whether a change affects the SSP, diagrams, asset inventory, responsibility matrix, or CUI-flow documentation.

Likewise, successful backup jobs do not prove recoverability. NorthStar standardizes restoration-test records that capture the customer, system or data tested, backup source, restore destination, technician, objective, timestamps, result, validation, problems, corrective action, and reviewer.

19.126 The Remediation Decision Worksheet

Field	Question
Problem	What exactly happened?
Security capability	What requirement or process is affected?
Current state	What happens today?
Desired state	What should happen?
Root cause	Why does the gap exist?
Customer responsibility	What must the defense contractor do?
MSP responsibility	What must the MSP do?
Provider dependency	Does another provider participate?
Corrective action	What will change?
Validation	How will we know it works?
Evidence	What records demonstrate completion?
Documentation impact	What needs updating?
Operationalization	How will the corrected process continue?

19.127-19.132 Building a Remediation Evidence Package

A disciplined evidence package can be organized by original issue, root-cause analysis, corrective action, implementation, validation, documentation, and final approval. The exact folder names are not CMMC requirements; the value lies in traceability.

Evidence names should be meaningful. A file such as HarborPoint_BackupRestoreTest_ENGFS01_2026-11-03.pdf communicates far more than Screenshot1.png. An evidence index can record an ID, description, source, owner, period covered, sensitivity, storage location, and reviewer.

Evidence ownership may span organizations. Beacon may generate the alert, NorthStar may own the related ticket, and Harbor Point may own the business decision. Responsibility planning should therefore include who produces, retains, retrieves, and provides each important record.

19.133-19.138 Detailed 30/60/90-Day Plan

Period	Primary Objective	Representative Actions
Days 1-7	Stabilize	Preserve records, identify deadlines, assign owners, remove temporary assessment access, review temporary rules and accounts
Days 8-30	Correct and understand	Root-cause analysis, remediation, documentation correction, inventory and access reconciliation, provider review
Days 31-60	Operationalize	Update procedures, ticket templates, recurring reports, onboarding/offboarding, change workflows, training
Days 61-90	Validate	Tabletop exercise, evidence sampling, restore test, access reporting test, SSP and responsibility-matrix verification

Day 90 is not another finish line. It marks the point where assessment lessons should have been absorbed into recurring operations.

By approximately Day 90, the organization should test the new operating model. Ask for the current privileged-access report and sample it against source systems. Trace a recent termination from business notification through access removal. Review a recent significant change and verify that documentation impact was considered. Perform a restore test and an incident tabletop.

The objective is not another mini-assessment. It is practical validation that the improvements are working during ordinary operations.

19.139-19.143 Level 1 Annual Readiness Workbook

Pine Valley Precision Components represents a small contractor that may have no full-time security staff and may depend heavily on an MSP. Its owner should be able to answer plain-English questions about the government-related information it handles, where that information is stored, who can access it, what systems are involved, what the MSP manages, what Pine Valley manages, and whether the safeguards still operate.

Activity	Pine Valley	MSP	Shared
Employee hiring/termination notification	Yes		
Account provisioning		Yes	
Access approval	Yes		
Firewall management		Yes	
Endpoint security		Yes	
Employee security behavior	Yes		
Backup administration		Yes	
Technology-change communication			Yes
Annual review			Yes

The value of this simple sheet is educational: it shows a small contractor that outsourcing IT does not outsource every CMMC responsibility.

19.144-19.150 Level 2 Continuous-Readiness Workbook

Harbor Point organizes recurring readiness into six operating areas: scope; identity and access; systems and configuration; security operations; evidence; and governance. Each area has an owner and review cadence.

A Level 2 environment may include many more systems, providers, identities, security tools, and CUI workflows. The multi-year assessment cycle can create a false sense that there is plenty of time before readiness matters again. In reality, three years is enough time for the environment to change dramatically.

Harbor Point therefore uses recurring reviews to keep scope, access, providers, vulnerabilities, monitoring, backup, incident response, documentation, and evidence aligned between assessment events.

- Scope: new locations, systems, cloud services, CUI flows, providers, network boundaries, remote work, and subcontractors.
- Identity and access: joiners, leavers, role changes, privileged users, service accounts, MSP technician assignments, and MFA exceptions.
- Systems and configuration: assets, configuration exceptions, patching, vulnerabilities, security-agent health, encryption, logging, firewall changes, and backup coverage.
- Security operations: alerts, incidents, escalation performance, unresolved security tickets, monitoring gaps, and threat patterns.
- Evidence: whether required records are produced, retrievable, protected, current, and customer-specific.
- Governance: risks, major changes, provider issues, incidents, remediation, scope changes, and documentation accuracy.

19.151 The Change-Impact Questionnaire

Question	Response
What is changing?	Describe technology, process, location, provider, or business change
Will FCI be affected?	Yes / No / Unknown
Will CUI be affected?	Yes / No / Unknown
New system or service?	Yes / No
Administrative access change?	Yes / No
External provider gains access?	Yes / No

Logging or monitoring changes?	Yes / No
Backup or recovery changes?	Yes / No
Network architecture changes?	Yes / No
SSP review needed?	Yes / No / Unknown
Responsibility matrix review needed?	Yes / No / Unknown
Asset inventory update needed?	Yes / No
Validation required?	Describe post-change validation

19.152-19.154 Applying Change Review

A new cloud collaboration platform may introduce CUI processing, external users, new logs, new administrative responsibilities, and a new provider. That is a security architecture decision, not merely a software purchase. By contrast, replacing a standard approved printer with the same model may require an asset update but not an extensive CMMC review. The process should be proportional.

The MSP should apply a parallel provider-change review to its own RMM, backup, security, identity, and management platforms, considering customer access, data handling, authentication, logging, isolation, evidence, and notification.

19.155-19.156 Technician Access Worksheets

Offboarding

- Corporate identity disabled and MFA revoked
- VPN removed
- PSA/RMM/password-vault access removed
- EDR/backup/SIEM access removed
- Customer cloud and firewall roles removed
- Local and emergency accounts reviewed
- Manager validates removal
- Customer-specific access register updated

Onboarding

- Business need identified

- Role and least privilege determined
- Required training completed
- Access approved
- MFA enforced
- Vault access configured
- Access recorded
- Responsibilities acknowledged
- Review date established

19.157 Annual Affirmation Preparation Package

Management should not be handed an affirmation screen and told to click it. An internal package should summarize the relevant CMMC status, scope, significant changes, security operations, privileged-access review, documentation status, provider changes, remediation, and management review. The purpose is informed governance.

Affirmation should be treated as a governance activity. Management does not need to inspect every technical setting, but the authorized official should receive enough current information to understand the organization's scope, major changes, significant open issues, provider changes, privileged-access status, documentation accuracy, and security operations.

An affirmation process that consists only of sending an executive a link and saying “click here” misses the purpose of informed organizational responsibility.

19.158-19.160 Continuous-Readiness Dashboard and Service Review

Operational Area	**Example Indicator**
Scope	Unreconciled assets; services awaiting review
Identity	Privileged users; MSP privileged technicians; MFA exceptions
Vulnerability	Critical and overdue vulnerabilities
Endpoint	Reporting endpoints; encryption coverage; unhealthy EDR agents
Backup	Protected systems; unresolved failures; restore-test currency
Security operations	Open critical incidents; monitoring gaps
Governance	High-priority remediation; SSP and responsibility-

	matrix status

A dashboard should tell management where attention is needed; it should not pretend to reduce CMMC to a simplistic percentage. Monthly MSP service reviews and deeper quarterly customer/MSP security reviews keep the shared operating model visible.

19.162-19.164 Internal Readiness and Evidence Sampling

Periodically sample real operations rather than only prepared examples. Select a terminated employee, newly deployed laptop, firewall change, critical vulnerability, restore test, and privileged technician. For each sample, trace the lifecycle from authorization through implementation, validation, and evidence.

> ***The Random Tuesday Test: Could we explain what happened on an ordinary day six months ago using dependable operational records?***

19.165-19.171 Provider Transition Scenario

If Harbor Point replaces NorthStar with Summit Technology Services, the transition should begin by inventorying NorthStar's responsibilities and evidence dependencies. Administrative access is transferred and revoked under control, security services are validated for continuity, and the SSP, responsibility matrix, provider records, and evidence ownership are updated.

A mature MSP exit package may include appropriate asset inventories, customer-specific configuration records, open security issues, documentation, approved customer records, access-transition information, and historical evidence as contractually appropriate. The defense contractor's security program should not collapse because its MSP relationship changes.

19.172-19.174 Evidence Retention and Management Review

Evidence retention should be based on applicable policy, contract, legal, operational, and assessment needs rather than an invented universal period. Evidence repositories may contain sensitive diagrams, administrator names, vulnerability details, or incident information and therefore require access control, protection, monitoring, retention, and secure disposal.

Evidence retention should be deliberate rather than unlimited. Security evidence may contain network diagrams, administrator names, vulnerability details, incident information, screenshots, configuration information, or CUI. The repository therefore deserves access control, monitoring, backup, and secure disposal practices appropriate to the information it contains.

The organization should retain records according to applicable contractual, legal, policy, operational, and assessment needs. The objective is to preserve what is needed without creating an uncontrolled archive of sensitive information.

Quarterly Management Review Agenda

202. Significant business changes
203. Scope changes
204. Security posture
205. Open remediation
206. Provider changes
207. Documentation accuracy
208. Upcoming assessment, affirmation, or contract obligations

19.175-19.180 Teaching the Customer/MSP Relationship

> ***The customer owns its obligations. The MSP performs defined technical and security responsibilities. Both must understand the handoffs.***

A defense contractor should ask a prospective MSP how technician access is controlled, how onboarding and offboarding work, whether customer-specific reports can be produced, how changes and incidents are documented, how vulnerabilities and backups are managed, how customer environments are separated, and how assessment evidence requests are supported.

An MSP should ask the contractor what contracts it supports, whether it handles FCI or CUI, where that information resides, which systems and providers are involved, whether an SSP exists, what responsibilities the customer expects the MSP to perform, what assessment status exists, and whether remediation remains open.

When a customer says 'Just make us compliant,' the MSP should explain that it can implement and operate many technical services, but the customer retains responsibilities involving contracts, information identification, personnel, physical processes, approvals, governance, and business decisions.

19.181-19.190 Training, Maturity, and Metrics

Post-assessment technician training should explain why customer-specific evidence, controlled access, meaningful tickets, temporary-change closure, security escalation, and tenant isolation matter. Customer employee training should emphasize approved systems, suspicious-activity reporting, CUI handling, access discipline, and how to contact IT/security. Executive training should focus on scope, risk, providers, remediation, resources, and affirmation.

A useful maturity progression is Reactive -> Scheduled -> Integrated -> Observable. First put recurring activities on a calendar. Then connect security to business events such as hiring, termination, procurement, and change. Finally create dashboards, exception reports, evidence indexes, and management reviews that reveal whether those processes are working.

Metrics should drive decisions. Unhealthy endpoints, overdue critical vulnerabilities, overdue access reviews, unresolved backup failures, and systems missing security agents are usually more actionable than impressive-sounding threat counts.

19.190 Continuous-Readiness Calendar

Cadence	Examples
Monthly	Security service review; critical vulnerability review; backup exception review
Quarterly	Privileged-access review; asset reconciliation; provider review; evidence sampling
Semiannual	Incident tabletop; selected restore testing; documentation review
Annual	Broader readiness review; training review; responsibility review; applicable affirmation preparation

19.191-19.195 The No-Surprises Principle and Operational Problems

The objective of continuous readiness is simple: no surprises.

The next assessment should not reveal a forgotten network, unknown administrator, unapproved cloud service, departed technician, undocumented provider, unmonitored server, or untested backup. Problems will still occur, but the organization should have processes capable of discovering and managing them.

Operational plans of action can help manage vulnerabilities or temporary deficiencies arising after implementation. They should not be confused with formal assessment POA&Ms or used as a general excuse for incomplete implementation.

19.196 Why Terminology Matters

Terms such as POA&M, OPA, SSP, OSC, ESP, C3PAO, and SPRS can make CMMC sound like another language. The teaching method throughout this book is therefore deliberate: teach the idea first, then teach the formal term and acronym. A reader who understands the concept can learn the acronym; memorizing the acronym without understanding the concept teaches very little.

19.197 Final Post-Assessment Master Checklist

- Preserve assessment records and schedule lessons learned.
- Record findings and assessment friction; identify deadlines and owners.
- Remove temporary assessment access and temporary rules.
- Define each remediation problem and root cause.
- Assign customer, MSP, and provider responsibilities.
- Implement, validate, preserve evidence, and operationalize the correction.
- Review SSP, diagrams, inventory, responsibility matrix, procedures, and CUI flows.
- Review privileged access, onboarding/offboarding, vulnerabilities, patching, monitoring, backup, incident escalation, and change management.
- Establish monthly, quarterly, management, evidence-sampling, and annual readiness reviews.

19.198-19.200 Defense Contractor, MSP, and Shared Self-Checks

Defense Contractor

- We know what information we protect and where it resides.
- We know which systems and providers support it.
- We know what our MSP performs and what remains ours.
- We know who has privileged access.
- We know how significant changes and incidents are handled.
- We know whether our documentation and evidence remain current.

MSP

- We know which customers have CMMC-related requirements.
- We know which services we perform for each customer.
- We control technician access and can report it by customer.
- We document significant changes and produce customer-specific evidence.
- We have repeatable onboarding/offboarding and incident escalation.
- We can support assessment requests without improvising or exposing other tenants.

Shared

- We agree about who does what.
- Our documents, technicians, systems, and evidence tell the same story.
- If an assessor asked us separately, our answers would align.

19.201-19.205 Final Chapter Perspective

The post-assessment period reveals whether CMMC was treated as a temporary compliance project or as an improvement to the way the organization protects information. Anyone can clean a room before an important visitor arrives. The more meaningful question is what the room looks like six months later.

> ***Defense contractor: your MSP can help enormously, but your organization must understand its own CMMC environment.***
>
> ***MSP: your customer may own the contractual obligation, but the way you operate technology may directly support that customer's ability to satisfy and demonstrate security requirements.***
>
> ***Both: the strongest operating model is customer + MSP + other service providers working from clearly defined responsibilities.***

Chapter 19 Final Conclusion

The assessment is over, but the program continues. Readiness is preserved by controlling change, operating dependable security processes, generating trustworthy evidence as a natural result of those processes, and maintaining clear responsibility across the contractor, MSP, and other service providers.

A vulnerability will appear. An employee will leave. A backup will fail. A security tool will stop reporting. A new cloud service will be requested. A technician will

make a mistake. A provider will change. The mature organization detects change, evaluates it, documents it, validates it, and learns from it. That is continuous readiness.

Regulatory note: CMMC program requirements can change. The regulatory statements in this edition were checked against current U.S. Department of Defense CMMC program materials and the official CMMC Frequently Asked Questions available in September 2026. Readers should verify current contract language and official DoD guidance when applying these requirements to a specific organization.

Transition to Chapter 20

Chapter 20 - Building CMMC into MSP Operations - moves inside the MSP and examines how CMMC-aware security becomes part of everyday service delivery: technician onboarding, customer onboarding, privileged access, PSA and RMM workflows, change management, patching, vulnerability management, backup, security monitoring, incident escalation, evidence generation, and technician training.

> ***Not as a sales offering. Not as a marketing label. Not as a compliance checkbox. But as an operating discipline.***

CMMC for MSPs: From Readiness to Certification

Chapter 20

Building CMMC into MSP Operations

Expanded Teaching Edition

Authored by Dr. Charles Edwards

A practical guide for MSPs and the defense contractors they support

Chapter Purpose

Chapter 20 moves the discussion from assessment preparation into the ordinary operating life of a managed service provider. The central idea is simple but demanding: a CMMC-ready environment cannot depend on a burst of activity before an assessment. Security has to be produced by normal work. The same processes that create accounts, deploy endpoints, approve software, patch systems, manage privileged access, respond to alerts, restore data, and close tickets must also preserve the discipline and evidence needed to explain how the environment is protected.

Throughout the chapter we continue with Harbor Point Engineering, its managed service provider NorthStar Managed Technology, and Beacon SOC. These organizations are fictional, but the operating problems are deliberately realistic. Harbor Point represents a defense contractor that must understand and govern its own environment. NorthStar represents the MSP that performs substantial portions of day-to-day IT and security operations. Beacon represents a specialized monitoring provider. Their relationship lets us examine an important CMMC truth: accountability can be distributed operationally without becoming vague. The customer still owns its obligations, while providers remain accountable for the services and actions assigned to them.

This chapter is written for the reader who may understand IT operations but not yet speak CMMC fluently, and for the reader who may understand CMMC requirements but has never run an MSP service desk. For that reason, each operational area is explained as a business process first, then connected to security, responsibility, evidence, failure modes, and continuous improvement. The goal is not to make every technician a compliance specialist. The goal is to make secure behavior the ordinary way work is performed.

20.1 When CMMC Becomes Ordinary Operations

An organization can look prepared for an assessment without being operationally mature. Policies can be rewritten, screenshots can be collected, stale accounts can be removed, and dashboards can be cleaned up in the weeks before an assessor arrives. Those activities may improve the environment, but they do not prove that security has become part of normal operations. A mature program behaves differently. On an ordinary Tuesday, the organization can explain who has access, which assets are expected, which protections are operating, which exceptions remain open, which changes occurred, and what happened when something failed.

For an MSP, this distinction is critical because service delivery never stops. NorthStar cannot place Harbor Point into a special compliance mode for several months and then return to ordinary behavior after the assessment. New employees will continue to arrive. Employees will leave. Software will change. Vendors will request access. Vulnerabilities will be discovered. Backups will fail. Security alerts will occur. Cloud services will evolve. The operating model has to absorb these events without losing control of authorization, responsibility, or evidence.

This is why the most useful question is not, “What evidence do we need for CMMC?” The better question is, “What reliable record should a well-run security process naturally create?” When NorthStar provisions an account from an authorized request, the authorization and provisioning record are evidence. When it patches an endpoint and verifies the result, the deployment and validation records are evidence. When Beacon escalates suspicious activity and NorthStar contains it, the alert, incident timeline, actions, and communications are evidence. Evidence becomes a by-product of disciplined operations rather than a separate compliance factory.

20.2 The Operating Model: Baseline, Service, and Customer Layers

NorthStar needs standardization because an MSP cannot scale if every technician invents a different way to perform routine work. At the same time, Harbor Point cannot be treated as interchangeable with every other customer. The practical answer is a layered operating model. NorthStar establishes an MSP-wide baseline for identity, technician behavior, privileged access, ticket quality, change control, endpoint administration, monitoring, backup handling, incident escalation, and evidence retention. Individual services then add their own procedures. Finally, each customer receives a customer-specific overlay that captures the distinctions that matter for that environment.

The customer-specific layer is where Harbor Point’s CUI environment, authorized contacts, approved applications, emergency authorities, maintenance restrictions, escalation paths, provider relationships, and special technical conditions become operationally visible. This layer should not attempt to duplicate the entire System Security Plan. It should translate the portions of that plan that affect service delivery into information an authorized technician can use while doing the work.

This layered approach solves two problems at once. NorthStar can standardize the majority of its operating behavior, which improves consistency and training, while preserving the customer-specific decisions that cannot safely be generalized. Chapter

21 will scale this model across many customers. For now, Harbor Point gives us the opportunity to examine the model deeply before we multiply it.

20.3 The Customer Security Profile

The Customer Security Profile is NorthStar's operational bridge between customer governance and technician execution. When Maria opens a Harbor Point ticket, she should not have to search through hundreds of pages of assessment documentation to learn whether a particular action requires customer approval. The profile should tell her what kind of environment she is entering, which systems are especially sensitive, which contacts can authorize access or changes, which applications and services are approved, how incidents are escalated, and where customer-specific procedures differ from NorthStar's baseline.

A useful profile also explains boundaries. Harbor Point may have systems that process or store CUI, systems that provide security protection, ordinary corporate systems, and services delivered by external providers. NorthStar needs enough context to avoid treating those categories as identical. The profile should therefore point technicians toward the correct procedure rather than encouraging them to make scoping judgments during routine ticket work.

The profile is valuable only if it stays current. A customer contact who left six months ago, an application that has moved to a new cloud service, or an obsolete escalation number can turn documentation into a source of error. NorthStar should therefore connect profile maintenance to onboarding, significant changes, quarterly reviews, provider changes, and customer offboarding. Documentation should follow reality, not merely describe the environment as it existed when the document was written.

20.4 New User Onboarding: Jordan Lee

Jordan Lee joins Harbor Point as an engineer. From the business perspective, onboarding seems simple: Jordan needs an account, a laptop, email, and access to engineering resources. From the security perspective, however, onboarding establishes a new identity, creates authentication credentials, assigns permissions, introduces an endpoint, connects that endpoint to management and security services, and grants access to information. A weak process treats these as separate technical tasks. A mature process treats them as one controlled lifecycle.

Harbor Point begins the process because Harbor Point owns the employment relationship and knows what Jordan is supposed to do. An authorized manager identifies Jordan's role, start date, required project resources, and any special access. NorthStar implements the approved access. This distinction matters. The MSP can technically create permissions, but the customer should determine the business need for those permissions. Customer authorization and MSP implementation are connected responsibilities, not interchangeable ones.

Maria verifies that the request came through the approved channel and matches Harbor Point's role model. She provisions Jordan using the Standard Engineering User profile rather than copying permissions from another employee. Copying a convenient user can silently reproduce excessive access accumulated over years. A role-based starting point is easier to understand, review, and maintain. Project-specific access is then added only where Harbor Point has authorized it.

Jordan's laptop follows a parallel process. The device is recorded, assigned, enrolled in the management environment, configured, patched, protected by the required endpoint-security mechanisms, and validated before delivery. The important word is validated. "Agent installed" does not necessarily mean "agent operational." NorthStar needs to know that the device is actually reporting to the systems expected to manage or protect it.

20.5 Authentication, Authorization, and Least Privilege

Authentication answers the question, "Are you the person you claim to be?" Authorization answers a different question: "What is that authenticated person permitted to do?" These concepts are often discussed together because identity platforms implement both, but operationally they must remain distinct. Jordan may authenticate successfully and still be denied access to a project folder because Harbor Point has not authorized that project access.

Least privilege does not mean making work unnecessarily difficult. It means providing the capability required for the job without granting broader authority merely for convenience. Jordan needs engineering applications and project resources. He does not automatically need permanent local-administrator rights. NorthStar can install approved software through managed deployment or controlled elevation without turning every application request into permanent administrative access.

The same principle applies to NorthStar technicians. Maria may need administrative access to Harbor Point endpoints because her assigned role requires it. She does not

therefore need unrestricted access to every Harbor Point system or every NorthStar customer. Privilege should follow responsibility. When responsibility changes, privilege should change with it.

20.6 The MSP Privileged-Access Lifecycle

Privileged access deserves lifecycle thinking because it is one of the most consequential capabilities an MSP holds. NorthStar begins by identifying which technician roles require which forms of customer administration. Maria's assignment to Harbor Point creates a business reason for access. That reason is approved, translated into specific permissions, and provisioned through the appropriate identity, RMM, documentation, and credential systems.

Where possible, privileged credentials should not become permanent knowledge carried in a technician's memory. A controlled credential or privileged-access mechanism can reduce unnecessary exposure, support rotation, and improve accountability. Shared administrative accounts deserve particular caution because they can obscure who actually performed an action. If a shared technical identity is unavoidable, the surrounding process should preserve individual accountability through controlled checkout, session records, or other appropriate mechanisms.

Periodic review is essential because privilege tends to accumulate quietly. A technician is added for a project, assists during an incident, covers another employee's vacation, and gradually retains access that no longer corresponds to the current role. NorthStar should therefore compare current access with current responsibility. The question is not whether Maria is trustworthy. The question is whether Maria still needs the capability.

Temporary elevation should remain temporary. If Maria needs broader server rights for an unusual repair, the record should explain why, who authorized it, what she did, and when the exceptional access ended. This converts least privilege from a policy statement into an operational behavior.

20.7 The RMM as an Administrative Control Plane

Remote monitoring and management technology gives an MSP extraordinary leverage. From one console, authorized personnel may inventory systems, deploy software, execute scripts, open remote sessions, modify configurations, and administer large portions of a customer environment. That efficiency is central to the

MSP business model, but it also makes the RMM a high-value administrative control plane.

NorthStar therefore has to secure the RMM as carefully as it expects Harbor Point to secure its own privileged systems. Technician identities, strong authentication, role design, customer separation, session accountability, logging, automation control, API credentials, and administrative workstations all matter. A compromise of the RMM can turn one provider incident into a multi-customer event.

The RMM also creates evidence. It can help establish which endpoints are enrolled, which scripts were executed, which software was deployed, and which technician performed certain actions. But the presence of logs does not automatically create useful evidence. NorthStar needs retention, customer-specific retrieval, time synchronization, and enough context to connect technical events to authorized work.

20.8 The PSA and Service-Management System as Security Infrastructure

The professional services automation or IT service-management platform is often thought of as a business system for tickets, billing, and service levels. In a CMMC-supporting MSP, it also becomes security-relevant infrastructure because it records authorization, changes, incidents, exceptions, and customer communications. ServiceNow is one example of a platform that can support structured request, incident, change, and workflow processes; many MSPs use other PSA or ITSM products. The function matters more than the brand.

A strong ticket tells an operational story. It identifies the request or condition, the relevant authorization, the work performed, exceptions encountered, validation completed, and final disposition. “Fixed issue” may be enough to make a queue smaller, but it is not enough to reconstruct a security-relevant decision months later. At the same time, ticket quality should not become an exercise in writing essays. The record should capture the facts another authorized person would need to understand what happened and why.

The PSA also needs protection because its records may contain internal addresses, architecture details, vulnerability information, incident notes, user information, or other sensitive operational data. Evidence should not be protected less carefully merely because it exists to prove that other systems are protected.

20.9 Password Vaults, Privileged Credentials, and Break-Glass Access

Credential management is one of the areas where MSP convenience can collide with customer risk. Technicians need timely access to systems they are authorized to administer, but distributing static passwords through documents, chat messages, or personal notes creates unnecessary exposure. NorthStar should use a controlled mechanism appropriate to the environment so that credentials can be restricted, rotated, audited, and removed as responsibilities change.

Emergency or break-glass access deserves special treatment. The purpose of emergency access is to preserve the ability to act when normal mechanisms fail, not to create a permanent shortcut around normal controls. NorthStar should define when emergency access may be used, who may use it, how use is recorded, how the customer is notified where appropriate, and what happens to the credential after use.

The vault itself becomes high-value infrastructure. If it exposes credentials across many customers, its identity controls, administrative roles, logging, recovery, and monitoring deserve serious attention. The MSP should never assume that because a security product stores passwords, the surrounding operating model is automatically secure.

20.10 Endpoint Lifecycle: From Arrival to Retirement

Endpoints do not become managed simply because an agent was installed once. A complete lifecycle begins when the device is acquired or accepted into the environment and continues through assignment, configuration, protection, maintenance, repair, reassignment, and retirement. Each transition can change who uses the device, what information it can reach, and whether its protections remain effective.

NorthStar should know the expected population of Harbor Point endpoints. This expected population becomes the reference against which RMM, endpoint-security, patching, and vulnerability-management populations can be compared. If Harbor Point has 118 endpoints but the endpoint-security platform reports 117, a dashboard showing 100 percent health for those 117 does not answer the real question. The missing endpoint is itself an exception requiring investigation.

Retirement matters just as much as deployment. A device leaving service may contain sensitive information, credentials, certificates, cached data, or management agents. NorthStar and Harbor Point need an appropriate process for data disposition,

removal from management systems, asset records, licensing, and any other dependencies. A retired device should not remain a ghost in dashboards or a forgotten path into the environment.

20.11 Software Installation, Application Control, and Approval

Software installation is one of the most common MSP activities, which is precisely why its security significance can be overlooked. A user asks for an application, a technician downloads an installer, administrative credentials are entered, the application launches, and the ticket closes. Yet the application may now open CUI, create temporary copies, synchronize data externally, install services or drivers, modify firewall behavior, require privileged execution, or introduce a new patching obligation.

Jordan’s request for specialized engineering software illustrates the correct sequence. NorthStar first determines whether the application is already approved. If it is not, Harbor Point confirms the business need while NorthStar evaluates the technical behavior. The team asks what information the application will process, whether it connects to cloud services, where data is stored, how updates occur, whether elevated privileges are required, and who will maintain the product. Software approval and software installation are therefore different decisions.

NorthStar obtains the approved installer from a trusted source rather than searching the web and executing the first download that appears. Maria performs controlled installation without granting Jordan permanent local-administrator rights. The application is configured, validated, entered into inventory, and placed into the patch and vulnerability lifecycle. Months later, when a vulnerability affects the installed version, NorthStar can identify the affected population because the software did not disappear into the environment after installation.

Current CMMC Level 2 assessment guidance addresses both controlling application execution and controlling and monitoring user-installed software. For an MSP, the practical lesson is that a policy becomes meaningful only when the organization can explain how authorized software is distinguished from unauthorized software and how the chosen approach is enforced and monitored. [1]

20.12 SaaS, Browser Applications, AI Services, and the Invisible Installation

Modern application control cannot stop at traditional installers. Jordan can open a browser, create an account with an online service, upload a file, and introduce an external processor into Harbor Point’s information flow without installing a single executable. The absence of an installer does not mean the absence of security impact.

This is especially important with artificial-intelligence services. An employee may want to summarize a document, analyze code, troubleshoot a configuration, or improve a report. The business value may be real, but the information entered into the service still matters. Harbor Point needs clear rules about approved services and permitted information. NorthStar technicians need the same discipline when troubleshooting customer systems. A firewall configuration, log extract, script containing secrets, or customer document should not be pasted into an unapproved service simply because doing so is convenient.

The broader operational category is therefore approved applications and services. Desktop software, SaaS, browser extensions, mobile applications, AI tools, cloud storage, collaboration platforms, and file-conversion websites can all participate in the information environment. The review process should follow the information and capability, not merely the presence of an installer.

20.13 Scripts and Automation Are Software

MSPs depend heavily on automation. PowerShell, Python, shell scripts, RMM components, API integrations, and orchestration tools allow a small team to manage large environments. The same leverage that makes automation valuable also makes mistakes scalable. A faulty script can create accounts, modify permissions, disable protections, or deploy software across hundreds of systems in seconds.

NorthStar therefore treats production automation as managed code rather than disposable technician convenience. The organization should understand who owns a script, where the authoritative version resides, what review is appropriate, which credentials or APIs it uses, how changes are introduced, and where it is permitted to run. A script copied from an Internet forum should not become production automation merely because it appears to solve the immediate problem.

Automation should also fail visibly. If a nightly job is expected to reconcile endpoint populations or create tickets for failed backups, NorthStar needs a way to notice when

the automation itself stops working. Otherwise, the organization may mistake silence for success.

20.14 Hardware, Peripherals, and Specialized Engineering Equipment

Software is not the only way an environment changes. A USB storage device, network printer, scanner, replacement drive, diagnostic appliance, specialized engineering instrument, or vendor-installed device can introduce new information paths and management responsibilities. A network printer may store documents internally. A scanner may transmit files by email or to a cloud service. A specialized instrument may run an embedded operating system that cannot accept the MSP's standard agents.

The same reasoning used for software applies. What is being introduced? Why is it needed? What information can it access? How does it communicate? Who manages it? How will it be maintained? What happens when it fails or reaches end of life? Does it alter the security boundary or create a new external-provider dependency? The answers determine the level of review required.

The objective is not to force every mouse and keyboard through a lengthy security committee. Good governance is proportional. A commodity peripheral with no meaningful security effect should not receive the same scrutiny as a network-connected engineering appliance with remote vendor access. The operating model should distinguish routine change from security-significant change.

20.15 Real Technologies in the Operating Model

Real MSP environments use real products, and readers benefit from seeing how product categories participate in operations. The safest way to teach this is to begin with the security function and then use vendors as examples rather than presenting products as compliance shortcuts. Microsoft and Okta can participate in identity and access architectures. CrowdStrike is an example of an endpoint-security platform. Splunk is an example of a platform used for security information and event analysis. Tenable is an example of vulnerability-management technology. ServiceNow can support service-management workflows. Kiteworks and PreVeil are examples of technologies organizations may evaluate for protected information exchange or collaboration scenarios.

These names do not create CMMC compliance. An organization can purchase excellent technology and still configure it poorly, fail to enroll assets, ignore alerts,

retain excessive privileges, or send sensitive information through an unapproved workflow. Technology provides capability. People, architecture, configuration, process, responsibility, monitoring, and evidence determine how that capability is used.

The integrated view is more useful than a product list. Jordan authenticates through the approved identity architecture. He works from a managed endpoint protected by endpoint-security controls. Relevant telemetry reaches the monitoring environment. Vulnerability technology identifies weaknesses. NorthStar records work in the service-management system. Sensitive information is exchanged through approved mechanisms appropriate to Harbor Point's architecture. The technologies form an operating system for service delivery rather than a shelf of unrelated products.

20.16 Change Management: The Connecting Tissue

Change management connects nearly every process in this chapter. A new application is a change. A firewall rule is a change. A patch is a change. A new cloud service is a change. Replacing the RMM is a change. Moving CUI into a new workflow is a change. The appropriate level of control should be proportional to the significance of the change.

Routine, low-risk, preapproved work should not require an executive meeting. Overly burdensome change control encourages bypass. At the other extreme, a major alteration to the platform through which NorthStar administers every Harbor Point endpoint deserves substantially more analysis than an ordinary workstation update. Good change management distinguishes standard, normal, and emergency changes and gives technicians a usable path for each.

The Friday firewall request shows why this matters. "Open the firewall for the vendor" is not enough information. NorthStar needs the business purpose, source, destination, service, duration, authorization, implementation detail, validation, and removal or review condition. A narrow, understandable rule is easier to defend and easier to remove than an emergency "any-to-any" exception that survives long after the project ends.

20.17 Major MSP Platform Changes

When NorthStar replaces its RMM, the change may look internal from a business perspective, but it directly affects how Harbor Point systems are administered. The new platform introduces identities, roles, agents, APIs, scripts, logging, customer

separation, and remote-control capabilities. NorthStar therefore evaluates the architecture before migration, defines how old and new populations will coexist, plans rollback, and identifies how to detect endpoints that appear in neither platform.

Harbor Point needs appropriate visibility when provider changes materially affect the services or architecture on which its security program depends. Current Level 2 scoping guidance states that significant architectural or boundary changes can require a new assessment, while operational changes within the existing assessment boundary that follow the existing SSP may be covered through continuing compliance mechanisms. The practical lesson is not that every tool change creates a new assessment. The lesson is that organizations should understand the security and scoping significance of material changes rather than assuming that provider technology is invisible to the customer. [2]

20.18 Patch Management Is an Exception-Management Process

Patch management is often described as a schedule: patches are released, tested, deployed, and reported. That description is incomplete. The difficult part of patching is what happens when the expected path fails. Harbor Point has 118 endpoints. A deployment succeeds on 114, two devices are offline, one update fails, and one engineering workstation cannot accept the update because of an application compatibility problem. A dashboard may still look overwhelmingly successful, but the security work now resides in the four exceptions.

NorthStar therefore manages patching by population and exception. The expected systems are known. Deployment occurs according to the defined process. Systems that do not reach the expected state are identified. Offline devices return to the queue when they reconnect. Failed installations are investigated. Compatibility conflicts receive business and technical review. Unsupported software is escalated as a lifecycle problem rather than hidden as a permanent patch failure.

Verification closes the loop. The fact that a deployment command was issued is not the same as proof that the system reached the intended state. NorthStar should use available management or vulnerability information to confirm remediation where appropriate. This distinction between action and outcome appears throughout mature operations.

20.19 Vulnerability Management: From Discovery to Verified Closure

A vulnerability scanner does not remediate vulnerabilities. It identifies conditions that require interpretation and action. NorthStar begins by determining whether a finding applies to the actual asset and configuration. It considers severity, exposure, exploitability, business role, available remediation, and operational constraints. The result is a prioritized work item rather than a raw scanner entry.

Suppose Tenable identifies a serious vulnerability in Harbor Point's engineering application. The vendor patch breaks a required workflow. NorthStar cannot responsibly declare the finding closed, but Harbor Point may not be able to accept immediate production disruption. The organizations document the condition, establish ownership, apply reasonable temporary protections, engage the software vendor, define a follow-up date, and keep the issue visible. When a compatible update becomes available, NorthStar deploys it and validates that the vulnerability condition is resolved.

Temporary protection is not the same as forgetting the vulnerability. The exception remains owned and reviewed. This is where ordinary operational exception management differs from the formal use of a CMMC assessment POA&M discussed in Chapter 19. Not every service ticket or risk item becomes an assessment POA&M, but unresolved security conditions still require disciplined operational management.

20.20 Backup Is Not Recovery

Backup dashboards are comforting because they reduce a complex process to a familiar green indicator. But the purpose of backup is not to create successful backup jobs. The purpose is to recover information and systems when needed. A backup program is therefore incomplete until restoration is exercised and validated.

When Harbor Point's engineering file-server backup fails, the alert should lead to investigation, correction, rerun, and verification. If the same workload fails repeatedly, NorthStar should recognize the pattern rather than treating each failure as an unrelated ticket. Trend review may reveal network instability, resource contention, a scheduling conflict, or an architecture that needs improvement.

During a restoration test, technical success is only one part of the result. Suppose NorthStar restores the data but Harbor Point engineers cannot open the files because permissions were not recovered correctly. The backup product may report success

while the business recovery outcome is still inadequate. The test should therefore validate usability at the level appropriate to the recovery objective.

20.21 Logging, Monitoring, and Beacon SOC

Logging creates records. Monitoring turns selected records into operational awareness. Beacon’s role is not simply to store Harbor Point telemetry. It analyzes activity, applies detection logic, investigates signals, and escalates events according to the agreed service. NorthStar then needs to understand what happens when Beacon escalates an event and which actions NorthStar is authorized to perform.

Coverage matters as much as alert quality. If Harbor Point expects twelve servers to send relevant logs and only eleven are reporting, the monitoring platform can appear healthy while a blind spot exists. NorthStar and Beacon therefore need a method for identifying expected sources and reconciling missing telemetry. The same expected-population principle used for endpoints and backups applies to logging.

Security monitoring also illustrates external-provider responsibility. Harbor Point may depend on Beacon for a portion of detection and analysis while depending on NorthStar for endpoint or identity response. The handoff between those providers is part of the control system. If Beacon can detect but cannot reach NorthStar, or NorthStar can contain but does not know when it is authorized to do so, the technical tools alone do not create an effective process.

20.22 The 2:13 a.m. Incident

At 2:13 a.m., Beacon detects suspicious privileged authentication associated with Harbor Point. The analyst reviews the available telemetry and determines that the event meets the agreed threshold for immediate escalation. At 2:18 a.m., Beacon notifies NorthStar through the established security escalation path. NorthStar’s on-call engineer acknowledges the alert and opens the Harbor Point incident record.

By 2:24 a.m., the available evidence indicates that the privileged identity may be actively compromised. NorthStar’s pre-established emergency authority permits the on-call engineer to disable the identity and terminate active sessions under defined circumstances. The engineer takes the action, records the time and rationale, and notifies Harbor Point’s designated incident contact. Beacon continues reviewing telemetry while NorthStar examines identity and endpoint information.

The team identifies resources accessed by the account, preserves relevant records, and searches for related indicators. At 3:07 a.m., enough information exists to provide Harbor Point leadership with an initial operational update. That update does not dump raw SIEM events on management. It explains what is known, what remains unknown, what actions have been taken, which systems may be affected, what business decisions are needed, and when the next update will occur.

Containment does not close the incident. Credentials and systems are reviewed, monitoring continues, recovery is validated, and Harbor Point considers information and contractual impact. After the immediate event, Harbor Point, NorthStar, and Beacon conduct a lessons-learned review. The final record therefore tells the complete story from detection through corrective action rather than preserving only the original alert.

20.23 Incident Escalation and Communication

A mature incident process distinguishes technical urgency from communication chaos. The team should know who is responsible for technical triage, who can authorize disruptive actions, who contacts Harbor Point management, who coordinates with external providers, and how evidence is preserved. These responsibilities should be established before the incident, because the worst time to negotiate emergency authority is while a privileged account may be under attacker control.

Communication should also match the audience. A SOC analyst needs detailed telemetry. A NorthStar engineer needs actionable technical context. Harbor Point leadership needs business impact, current containment status, unresolved questions, decisions required, and the next update time. Translating technical events into decision-quality information is an important MSP capability.

20.24 Personnel Security and Technician Lifecycle

MSP personnel changes can affect many customers at once. A new technician may need access to selected environments. A temporary technician may require narrower permissions. A technician changing teams may no longer need a customer. A departing employee may have accumulated customer-specific accounts over years. NorthStar therefore needs a personnel-access lifecycle that extends beyond disabling a single corporate identity.

When Maria moves into an internal role, her Harbor Point RMM permissions, customer-specific vault access, PSA visibility, and any other assigned privileges are reviewed and removed where no longer needed. The process occurs because her job changed, not because NorthStar distrusts her. Least privilege follows responsibility.

David's departure is more complex because he supported many customers. NorthStar disables corporate access, VPN, RMM, PSA, vault, cloud roles, and other central services at the appropriate time. It also identifies customer-specific accounts, reviews credentials known to David, reassigns open work, and verifies that critical customer knowledge remains in organizational documentation. Offboarding must reach the edges of the access model, not stop at the directory account.

20.25 Technician Training for Real Work

Technicians do not need to memorize every CMMC assessment objective to support a CMMC customer effectively. They do need to understand the decisions that appear in their work. Maria should know why she cannot grant local administrator rights merely to make an installation easier. She should recognize that a new cloud application may change where customer information goes. She should know that an urgent firewall request still needs defined authorization and scope. She should understand why customer information should not be pasted into an unapproved AI service.

Training becomes more useful when it follows realistic service scenarios. A password reset can teach identity verification. A software request can teach application approval and privilege. A failed patch can teach exception management. A security alert can teach escalation. A technician reassignment can teach least privilege. The goal is to make secure reasoning part of professional practice rather than a yearly presentation technicians click through and forget.

20.26 Remote Support and the Technician Workstation

Remote support changes physical location but not security responsibility. Maria may work from NorthStar's office or from an approved remote location, yet her workstation can still reach customer systems, the PSA, RMM, credential platform, documentation, and security consoles. That workstation occupies a position of trust and should be managed accordingly.

The more powerful the administrative capability, the more carefully the pathway to that capability should be protected. NorthStar should consider device management,

authentication, session controls, logging, network access, and the handling of customer information during troubleshooting. “Working from home” should not quietly become “working outside the operating model.”

20.27 Multi-Tenant Platforms and Customer Separation

An MSP gains efficiency by using platforms that contain many customers. The RMM, PSA, credential system, documentation platform, and monitoring environment may all be multi-tenant. That design creates an obligation to preserve customer separation. A Harbor Point technician should not accidentally expose another customer’s information in a screenshot, report, export, or support session.

Consider a seemingly harmless evidence request. Harbor Point asks NorthStar to show endpoint status. Maria opens a console and captures a screenshot that also reveals the names of seventy-four other customers in the navigation pane. The Harbor Point evidence may be technically accurate, but the method has exposed information belonging to others. Evidence preparation therefore needs the same customer-separation discipline as ordinary service delivery.

Role design, filtered views, customer-specific exports, naming conventions, report templates, and technician training can reduce this risk. Chapter 21 will examine multi-customer separation in much greater depth, but the operating principle begins here: efficiency must not erase boundaries.

20.28 External Service Providers and Shared Responsibility

NorthStar itself may depend on external service providers. Beacon provides monitoring. Cloud platforms may host management systems. Backup services may store protected data or security information. Identity and collaboration services may participate in the environment. Current Level 2 scoping guidance states that an ESP can be within scope when the applicable criteria are met and that the relationship and services should be documented in the OSA’s SSP, with provider service descriptions and customer responsibility matrices used to understand responsibility. [2]

The practical lesson is that provider responsibility should not be assumed. Harbor Point should know what NorthStar performs. NorthStar should know what Beacon performs. Each organization should understand the handoffs. If NorthStar says, “Beacon handles monitoring,” that statement is incomplete unless NorthStar also knows what sources Beacon receives, what Beacon investigates, when Beacon escalates, who responds, and what records are retained.

Shared responsibility is not a way to make accountability disappear. It is a way to divide a complex operating system into understandable responsibilities. The more providers involved, the more important those boundaries and handoffs become.

20.29 Evidence Follows Responsibility

A useful evidence principle is that evidence should follow the responsibility being demonstrated. If Harbor Point authorizes access and NorthStar implements it, the complete story may require both the customer authorization and the MSP provisioning record. If Beacon detects an event and NorthStar contains it, evidence may span the SOC alert, NorthStar incident record, technical action logs, and Harbor Point communications.

This is why asking one provider to “send all the CMMC evidence” is often the wrong request. No single provider necessarily owns the entire implementation story. The customer needs to understand where evidence originates and how the pieces connect. NorthStar can make this easier by maintaining an evidence map that identifies authoritative systems and retrieval methods without duplicating every record into a separate repository.

20.30 Evidence Retrieval as an Operational Capability

NorthStar should periodically test whether it can retrieve customer-specific evidence. Harbor Point might ask which NorthStar personnel currently have privileged access, which significant firewall changes occurred last quarter, which endpoints failed the latest patch cycle, when the last restoration test occurred, or which security incidents required escalation. The answer should not depend on searching personal notes or asking the one technician who remembers.

Reproducibility matters. If NorthStar produces a privileged-access report today, it should understand the source, filter, date, and scope well enough to produce a comparable report later. This reduces assessment stress and improves ordinary governance. Evidence retrieval becomes another service capability rather than a last-minute scavenger hunt.

20.31 The Dangerous Green Dashboard and Population Reconciliation

Dashboards summarize what a system knows. They do not necessarily reveal what the system is missing. NorthStar’s RMM reports 118 Harbor Point endpoints. The endpoint-security platform reports 117. The vulnerability scanner reports 116. The

asset inventory lists 119. None of these numbers should automatically be declared correct or incorrect without understanding the expected population for each function.

Perhaps one newly deployed laptop has not completed endpoint-security enrollment. Perhaps two isolated systems are intentionally outside a scanner’s network reach but are assessed through another method. Perhaps a retired device remains in the asset inventory. The discrepancy is the signal. NorthStar reconciles expected populations rather than selecting whichever dashboard looks best.

This idea is foundational because many security failures hide in absence. The system that never reported does not create an alert about its missing telemetry. The server omitted from backup cannot produce a failed backup job. The endpoint absent from the vulnerability scanner cannot report vulnerabilities. Knowing what should exist is therefore as important as analyzing what does exist.

20.32 Operational Exceptions Need Owners

Every mature environment has exceptions. A specialized application cannot yet be patched. A device is temporarily offline. A vendor requires time-limited access. A server cannot run the preferred security agent. An endpoint has a compatibility problem. The existence of an exception does not automatically mean the security program has failed. The more dangerous condition is an exception with no owner, no rationale, no review date, and no visibility.

NorthStar therefore treats exceptions as managed conditions. The record explains what expected state is not being met, why, who owns the next action, what temporary protection exists where appropriate, when the condition will be reviewed, and what would constitute closure. This prevents a thirty-day exception from quietly becoming a three-year architecture decision.

20.33 Metrics That Lead to Decisions

An MSP can measure almost anything, but useful metrics should lead to action. “4,721 patches installed” may sound impressive, yet Harbor Point may care more about which expected systems remain unpatched beyond the approved window and why. “99.2 percent backup success” is less useful than knowing which critical workloads have recurring failures and whether recovery has been tested.

Security-monitoring volume has the same problem. Thousands of alerts processed do not tell management whether meaningful threats were detected and handled.

NorthStar should therefore distinguish operational throughput from security outcomes. Metrics should help management see unresolved risk, recurring failure, coverage gaps, aging exceptions, and trends that require decisions.

20.34 Daily, Weekly, Monthly, and Quarterly Rhythms

CMMC becomes sustainable when important activities have a rhythm. Daily operations handle user requests, endpoint alerts, failed jobs, security escalations, and routine changes. Weekly review can surface aging exceptions, failed deployments, recurring backup problems, stale tickets, and unresolved vulnerabilities that individual technicians may not see as a pattern.

Monthly customer review translates technical operations into management understanding. NorthStar discusses meaningful changes, unresolved vulnerabilities, backup and recovery status, incidents, privileged-access changes, significant exceptions, upcoming lifecycle risks, and customer decisions that remain pending. The meeting should not become a slide show of vanity metrics. Its purpose is governance.

Quarterly review challenges assumptions. Do asset inventories still reflect reality? Does CUI still move where documentation says it moves? Have new providers or SaaS services appeared? Have temporary firewall rules survived beyond their purpose? Have administrative roles accumulated? Have applications changed architecture? Does the responsibility matrix still match service delivery? These questions help identify drift before an assessor does.

20.35 New Customer Onboarding: Meridian Defense Components

NorthStar’s experience with Harbor Point becomes the foundation for onboarding Meridian Defense Components, but NorthStar does not simply copy Harbor Point’s configuration. Meridian has different business processes, systems, providers, and information flows. NorthStar begins with discovery: what information Meridian handles, where FCI and CUI reside, which systems and users participate, how remote access works, what cloud services exist, which providers have access, how backups operate, and which unsupported technologies remain.

NorthStar wants Meridian to adopt its standard stack, but discovery comes before transformation. The MSP cannot safely standardize an environment it does not understand. During discovery, NorthStar finds unmanaged endpoints, former employees with active accounts, an unsupported server, users with local administrator

rights, untested backups, and an unsanctioned cloud-storage workflow. Some urgent conditions require immediate action, but the initial state is also documented so that later improvements can be distinguished from inherited conditions.

Onboarding eventually needs an exit condition. Meridian should not remain in an indefinite project state with temporary exceptions scattered across old tickets. Remaining issues are transferred into normal operational ownership, responsibility is confirmed, and the customer enters steady-state service with a known environment and known open conditions.

20.36 Customer Offboarding and Secure Transition

Customer offboarding deserves the same discipline as onboarding. Ending a commercial relationship does not automatically remove technical access. NorthStar reviews administrative identities, management agents, integrations, credentials, monitoring, backup responsibilities, documentation, open incidents, open vulnerabilities, and customer data held within provider systems. The receiving provider may need information necessary for continuity, and Harbor Point needs to understand exactly when responsibilities transfer.

A mature MSP should be able to help a customer leave securely. Security should not depend on customer captivity. NorthStar provides expertise and operational capability, but Harbor Point should retain enough ownership, documentation, and governance to transition responsibly if the relationship changes.

20.37 The MSP CMMC Operations Playbook

The playbook is the operational expression of everything taught in this chapter. It is not a substitute for the SSP, policies, contracts, responsibility matrix, or technical architecture. It tells authorized personnel how those higher-level decisions affect recurring work. A good playbook covers customer onboarding, technician onboarding, user lifecycle, endpoint lifecycle, privileged access, software and service approval, hardware changes, change management, vulnerability handling, patching, backup and recovery, logging and SOC escalation, incident response, evidence retrieval, recurring reviews, MSP platform changes, technician offboarding, and customer offboarding.

Each playbook procedure should answer the same practical questions. What starts the process? Who is authorized to request or approve the work? What does the MSP perform? What does the customer perform? Which provider handoffs exist? What

record is created? What happens when the normal path fails? How is completion verified? Who owns an unresolved exception? How is the process reviewed over time?

The playbook should be concise enough to use while the detailed chapter, policies, and procedures remain available for explanation. This is why we waited until the end of the teaching before summarizing. A checklist is powerful only when the people using it understand what the steps mean.

20.38 Worked Operational Record: New User

A well-written Jordan Lee onboarding record would identify the authorized requester, start date, approved role, project-specific access, assigned endpoint, required authentication, endpoint-management status, security-tool enrollment, and validation performed before handoff. It would record deviations rather than silently skipping them. If a required application could not be deployed, the ticket would remain linked to an owned exception instead of being closed as though onboarding were complete.

The value of the record is traceability. Months later, Harbor Point can understand why Jordan received his access and NorthStar can show how the authorization became technical implementation. The record is not good because it is long. It is good because it preserves the decisions another authorized person would need to reconstruct the event.

20.39 Worked Operational Record: Privileged Access

Maria’s privileged-access record identifies her assigned Harbor Point role, the administrative capabilities required, the approver, the systems or platforms involved, the date access began, and any customer-specific training or acknowledgement required. Temporary elevation is recorded separately from standing access. Periodic review confirms that the privilege still corresponds to her responsibilities.

When Maria changes roles, the same record helps NorthStar identify what must be removed. This is the advantage of lifecycle records: the information created during provisioning supports review and offboarding later.

20.40 Worked Operational Record: Firewall Change

The firewall-change record identifies the requester, business purpose, source, destination, protocol or service, expected duration, authorization, implementation

details, validation result, and review or expiration condition. If the change is emergency work, the record also identifies the emergency authority used and the required follow-up review.

Six months later, a reviewer should be able to determine why the rule exists without reverse-engineering its purpose from addresses and ports. If the project ended and the rule remains, the discovery should lead not only to removal but also to analysis of why the expiration mechanism failed.

20.41 Worked Operational Record: Vulnerability Case

The vulnerability record begins with the finding and affected asset, then documents validation, relevance, priority, remediation path, operational constraints, temporary protections, ownership, due or review date, deployment result, and final verification. If the vendor patch breaks production, that fact becomes part of the managed risk story rather than a reason to abandon the ticket.

The final closure should explain why NorthStar believes the condition is resolved. A scanner result, version check, configuration validation, or other appropriate evidence may support that conclusion. Closure is based on verified outcome, not simply on effort expended.

20.42 Worked Operational Record: Backup Restoration

The restoration record identifies the protected workload, backup set, test objective, restore location, start and completion time, technical result, business validation, problems discovered, corrective actions, and final disposition. If the files restore but permissions prevent authorized users from opening them, the test has revealed a recovery problem even though the backup software reports success.

The record becomes especially valuable when compared over time. Repeated restoration delays or recurring permission problems can reveal systemic weaknesses that individual successful backup jobs would never show.

20.43 Worked Operational Record: Incident Timeline

The Harbor Point incident record captures the sequence from Beacon detection through NorthStar acknowledgement, validation, containment, customer notification, evidence preservation, investigation, recovery, and lessons learned. Time matters

because it helps the organizations understand what was known at each stage and why particular actions were taken.

A useful incident timeline separates facts from hypotheses. At 2:24 a.m., the team may have suspected credential compromise without yet knowing the entry path. Later evidence may confirm or disprove that hypothesis. Preserving that distinction makes the record more accurate and more useful for future improvement.

20.44 Worked Operational Record: Technician Offboarding

David’s offboarding record extends beyond his primary corporate account. It identifies central platforms, customer-specific accounts, cloud roles, VPN, RMM, PSA, vault, documentation access, emergency credentials, open tickets, and any other assigned capability. Each relevant item receives an action and verification. Knowledge transfer is treated as part of continuity rather than left to informal memory.

The completed record should allow NorthStar to state with reasonable confidence that David no longer possesses active organizational access that his former role provided. That confidence comes from a defined population and verified actions, not from assuming that disabling one identity reached every customer system.

20.45 Worked Operational Record: Monthly Customer Security Review

The monthly Harbor Point review summarizes meaningful security state rather than overwhelming management with platform data. NorthStar explains endpoint coverage exceptions, significant vulnerabilities, backup and recovery concerns, important changes, incidents, privileged-access changes, aging exceptions, lifecycle risks, and decisions requiring Harbor Point input. Open items receive owners and follow-up dates.

The record of the meeting is itself useful governance evidence because it shows that the customer and provider are not operating in isolation. More importantly, it improves service. Problems that remain invisible inside technical queues become visible to the people who can make business decisions.

20.46 What the Defense Contractor Should Expect from Its MSP

Harbor Point should expect NorthStar to perform the services it has accepted responsibility for in a controlled and understandable way. That includes maintaining appropriate technician access, following customer-specific procedures, protecting provider administrative systems, managing exceptions, communicating material conditions, preserving operational records, and supporting evidence retrieval for the services it performs.

Harbor Point should not expect NorthStar to become the owner of every CMMC obligation merely because NorthStar operates important technology. The customer still needs to understand its environment, authorize business access, govern information use, maintain accurate scope and documentation, make risk decisions, train its people, and oversee providers. Outsourcing operations does not outsource accountability.

20.47 What the MSP Should Expect from the Defense Contractor

NorthStar also needs Harbor Point to participate. The MSP cannot maintain accurate access if the customer does not report role changes. It cannot protect a cloud application it does not know exists. It cannot remove a temporary vendor rule if nobody communicates that the project ended. It cannot determine business authorization for CUI use by guessing.

The healthiest relationship therefore includes timely customer decisions, accurate information, defined contacts, participation in reviews, and clear escalation. Shared responsibility works when both parties understand that a handoff has two sides.

20.48 Do Not Promise Certification

An MSP should be careful about language suggesting that its service makes a customer “CMMC compliant” or guarantees certification. NorthStar can describe the security functions it performs, the processes it follows, the evidence it provides, and the responsibilities it accepts. Harbor Point can use those services as part of its overall program. Assessment conclusions depend on the applicable requirements, scope, implementation, evidence, and assessment process, not on a marketing phrase.

Precise language protects both organizations. “NorthStar manages Harbor Point endpoint patching according to the documented service and provides operational

evidence" is far more meaningful than "NorthStar handles CMMC." The first statement can be tested against reality. The second hides responsibility.

20.49 Deep Operational Walkthrough: A Full NorthStar Workday

To see how the operating model behaves under ordinary pressure, follow NorthStar through a full workday. At 7:42 a.m., the service desk receives an automated notice that one Harbor Point endpoint has stopped reporting to endpoint security. At 7:51 a.m., an engineer submits a password-reset request. At 8:06 a.m., Harbor Point HR submits an onboarding request for a new employee starting the following Monday. At 8:19 a.m., the vulnerability platform identifies a high-severity condition on an engineering server. None of these events is unusual. Their importance comes from the way NorthStar decides what each event means and how it moves through the operating system.

The missing endpoint does not immediately become an incident. NorthStar first compares the device with the expected asset population and discovers that the laptop was assigned to an employee traveling overseas. The RMM also stopped reporting at approximately the same time. That correlation changes the investigation. The technician checks the approved travel information and contacts the user through the established channel. The device is powered off in transit. The exception is documented and a follow-up is scheduled. The team did not treat absence as success, but it also did not manufacture an emergency from incomplete information.

The password reset follows a different path. The technician does not rely solely on the caller knowing an employee number or manager name. NorthStar follows the approved identity-verification method before resetting the credential. The reset forces the expected authentication behavior, and the ticket records the verification method at an appropriate level without storing unnecessary secrets. A routine service-desk action has therefore protected the identity system rather than becoming a social-engineering shortcut.

The onboarding request enters a scheduled workflow because the start date is known. NorthStar confirms the approved role, prepares the endpoint, stages required software, and ensures that the identity will not become usable earlier than intended. Meanwhile, the vulnerability on the engineering server is validated and routed to the application owner because patching may affect production. Four different events entered four different processes, yet each process uses the same operating principles:

known trigger, appropriate authority, defined responsibility, recorded action, exception handling, and verified completion.

20.50 Password Resets, Help-Desk Identity Verification, and Social Engineering

Password resets deserve more attention than their apparent simplicity suggests. A help desk can possess the technical authority to take control of a user identity. If an attacker can persuade a technician to reset a password or alter an authentication method, the attacker may bypass protections that would otherwise prevent account compromise. For this reason, the reset process should be designed as an identity-verification process rather than merely a technical command.

NorthStar and Harbor Point establish acceptable verification methods before the urgent call arrives. The method should be strong enough for the risk of the account and practical enough that technicians will actually follow it. The exact design can vary, but the process should avoid easily discovered facts as the sole proof of identity. A manager callback, approved identity workflow, established secondary channel, or other appropriate mechanism may be used depending on the environment. The technician should also recognize situations that require escalation, such as a caller demanding that MFA be removed immediately or asking that the reset be sent to a new personal address.

The ticket should record that verification occurred and which approved method was used without turning the ticket into a repository for sensitive authentication data. This distinction is important. Evidence that the process was followed is useful; storing secrets in the evidence system is not. The reset event can also be correlated with identity logs when unusual circumstances exist, particularly if the request followed suspicious authentication activity.

This is another example of making the secure path the easy path. If the approved reset procedure takes thirty minutes while an informal chat message takes thirty seconds, technicians will experience pressure to bypass the procedure. NorthStar should therefore design an efficient verification workflow and train customer personnel on what to expect. Security improves when the correct process is both understood and usable.

20.51 Local Administrator Requests and Controlled Elevation

Local administrator rights are often requested because they solve immediate friction. An engineer needs to install a driver, a developer needs to update a tool, or a vendor insists that its application requires administrative execution. Granting permanent local administrator rights can make the ticket disappear quickly, but it also expands what the user and any process running under that user context can change.

NorthStar begins by identifying the actual requirement. Does Jordan need administrative capability every day, or does he need one approved installation? Can the application be packaged centrally? Can a controlled elevation mechanism provide temporary privilege? Can the vendor requirement be narrowed? The objective is not to reject legitimate work. It is to avoid turning a narrow operational need into broad permanent authority.

When temporary elevation is used, the record should explain the purpose and duration. If a role truly requires standing administrative capability, Harbor Point and NorthStar should make that an explicit role decision rather than allowing privilege to accumulate ticket by ticket. Periodic review can then compare the approved privileged population with the actual population.

This approach also improves troubleshooting. If a workstation unexpectedly has a local administrator that is not part of the approved population, NorthStar has a clear exception to investigate. Without an expected state, the same condition may remain invisible for years.

20.52 The Unsupported Server Problem

Harbor Point eventually discovers a server supporting an older engineering workflow that the vendor no longer supports. The server still works, which makes replacement difficult to prioritize. Engineers depend on it, the application cannot easily be migrated, and the business has deadlines. From an operational perspective, this is exactly the kind of condition that tests whether security governance can coexist with mission requirements.

NorthStar first makes the condition visible. The server is not allowed to disappear into an “old systems” category. The team identifies the business owner, technical dependency, information handled, network exposure, authentication model, backup status, monitoring coverage, and realistic replacement options. Where the system

cannot be immediately retired, Harbor Point makes an informed decision about interim protection and a migration path.

The important point is that unsupported does not mean unmanaged. NorthStar may reduce exposure, restrict access, improve monitoring, isolate the system where practical, ensure recovery capability, and limit unnecessary services while the replacement project proceeds. Those actions do not magically make unsupported software equivalent to supported software. They reduce risk while the organization works toward a sustainable state.

The exception should have an owner and recurring review. If the replacement date slips, that fact should be visible. If the vendor changes its support position, the plan should be updated. If the server begins processing new information or becomes reachable from a new network path, the risk picture changes. Operational maturity means continuing to manage the condition rather than treating the first risk discussion as the final answer.

20.53 Cloud Services, Shadow IT, and Information Flow

A department can introduce a cloud service faster than an MSP can deploy a server. A manager purchases a subscription with a credit card, invites several employees, and begins sharing documents. From the business perspective, the team solved a collaboration problem. From the security perspective, Harbor Point may have created a new identity system, information repository, external provider relationship, and data path without realizing it.

NorthStar should therefore build discovery into normal operations. Identity logs, endpoint observations, browser or network telemetry where appropriate, expense and procurement processes, customer conversations, and periodic reviews can all reveal services that were not part of the documented architecture. Discovery should not begin with punishment. The first questions are what business problem the service solved, what information entered it, who has access, how authentication works, and whether the service can be brought into an approved architecture or should be removed.

This is particularly important when CUI may be involved. The question is not simply whether the cloud vendor has good security marketing. Harbor Point needs to understand whether the service is appropriate for the intended information and how it affects its obligations and scope. NorthStar can provide technical analysis, but Harbor

Point retains the business and contractual responsibility for deciding how its protected information is handled.

Shadow IT is often a symptom of friction. If employees repeatedly bypass the approved collaboration system, the organization should ask whether the approved method is unavailable, poorly understood, or operationally impractical. Security improves when the organization addresses the underlying need while maintaining appropriate protection.

20.54 Secure Information Exchange in Daily Operations

Defense contractors routinely exchange files with customers, subcontractors, engineering partners, and government organizations. The transfer method is therefore not an occasional edge case; it can be part of daily operations. Harbor Point and NorthStar need to know which mechanisms are approved for which information and how users should behave when a partner requests a different method.

Technologies such as Kiteworks or PreVeil may be evaluated as part of secure information-exchange architectures, just as other organizations may use different products. The product name does not answer the operational questions. NorthStar still needs to understand identity, access, sharing permissions, external recipients, retention, administrative roles, logging, endpoint behavior, and the information types the workflow is intended to support.

A common failure occurs when an approved platform exists but users fall back to ordinary email or consumer file sharing because the approved workflow feels inconvenient. Harbor Point should therefore train employees using realistic exchange scenarios and make the approved method accessible. NorthStar support personnel should know how to help users without suggesting shortcuts that bypass the intended protection.

Evidence of a functioning exchange process may come from configuration, access records, approved procedures, user training, service documentation, and operational logs. The objective is to demonstrate that the organization understands how protected information leaves one trusted location and reaches another, rather than merely showing that a secure-transfer product was purchased.

20.55 Security Protection Data and the MSP’s Own Exposure

MSPs sometimes focus so strongly on CUI that they underestimate the sensitivity of security protection data. Configuration information, logs, vulnerability findings, network diagrams, identity records, administrative metadata, and security alerts may reveal how a customer environment is protected or where it is weak. Even when a particular record is not itself CUI, its compromise can materially increase risk.

NorthStar therefore considers where this information resides. The PSA may contain vulnerability descriptions. The documentation platform may contain network diagrams. The SIEM may contain authentication and endpoint telemetry. The credential platform contains privileged secrets. Backup consoles reveal system names and recovery architecture. These systems deserve protection appropriate to the role they play.

Current Level 2 scoping guidance specifically recognizes Security Protection Assets and notes that external providers may be relevant when CUI or Security Protection Data resides on provider assets under the applicable criteria. [2] The operational lesson is broader than terminology: the MSP should understand the security consequence of the data its own platforms aggregate.

This also affects evidence exchange. NorthStar should not casually email a vulnerability export containing internal addresses and exploitable conditions merely because Harbor Point requested “the report.” The method of delivering evidence should reflect the sensitivity of the evidence itself.

20.56 Configuration Baselines and Drift

A configuration baseline describes the expected state from which meaningful deviation can be recognized. Without a baseline, technicians can identify obvious failures but may not know whether a setting is intentionally different or simply drifted over time. Harbor Point’s endpoint baseline might address required security tooling, encryption, authentication behavior, approved services, update configuration, logging, and other settings appropriate to the environment.

Drift is normal because systems are operated by people and software. Applications update, technicians troubleshoot, vendors change defaults, and business needs evolve. The goal is not to create a frozen environment. The goal is to distinguish authorized evolution from uncontrolled change. Some drift should be corrected; some should be approved and incorporated into a revised baseline.

NorthStar can use management platforms to detect portions of configuration state, but tooling does not eliminate the need for interpretation. A setting may be technically different because Harbor Point has an approved engineering exception. Another difference may reveal that a technician made a temporary troubleshooting change and forgot to restore the baseline. The record surrounding the change provides the context the dashboard cannot.

Quarterly review should therefore include meaningful baseline exceptions and recurring drift. If the same setting is repeatedly changed for legitimate operational reasons, the baseline or procedure may need improvement. Security controls should evolve with the environment rather than forcing technicians to repeatedly fight an obsolete standard.

20.57 Time, Logs, and the Ability to Reconstruct Events

Operational evidence becomes difficult to correlate when systems disagree about time. An identity event appears at 2:13 a.m., an endpoint alert at 2:17, and a firewall record at 1:18 because one system is using a different time zone or has inaccurate synchronization. During an incident, those discrepancies can obscure sequence and causality.

NorthStar should therefore understand time configuration across the systems that contribute important security records. The objective is not merely aesthetic consistency. Reliable timestamps help investigators establish what happened first, which account was active, whether a change preceded an alert, and how quickly the team responded. They also make evidence from multiple providers easier to reconcile.

Retention matters for the same reason. A customer may ask about an event months after it occurred. If one platform retains ninety days while another retains a year, the evidence available will differ. NorthStar should know the retention characteristics of systems on which its service depends and avoid promising historical evidence that the underlying platform does not preserve.

This knowledge belongs in service design and evidence planning. The right question is not “Do we have logs?” but “Which logs matter, where are they stored, how long are they retained, who can access them, and can we retrieve customer-specific records when needed?”

20.58 Evidence Quality: Screenshots, Exports, Tickets, and Demonstrations

Not all evidence has equal explanatory value. A screenshot can show a configuration at a moment in time, but it may omit scope, date, or population. An export can provide a broader population but may require explanation of fields and filters. A ticket can show authorization and work performed but may not independently prove the resulting technical state. A live demonstration can show current behavior but may not establish historical consistency.

NorthStar should therefore think in terms of evidence combinations. For Jordan's onboarding, the authorized request explains why access was granted, identity records show implementation, endpoint records show device enrollment, and the ticket connects the steps. For vulnerability remediation, the scanner identifies the condition, the ticket records analysis and action, and a later scan or validation establishes closure.

Evidence should also be understandable outside the tool that created it. An assessor or Harbor Point manager may not know NorthStar's internal field names. Reports should preserve enough context to explain customer, date, scope, and meaning. This is another reason to test evidence retrieval before assessment preparation begins.

The strongest evidence is often ordinary evidence. When records are created consistently during normal work, they are less likely to be reconstructed from memory. That improves both credibility and operational usefulness.

20.59 What Happens When a Procedure Does Not Work

A procedure can be formally correct and operationally unusable. Suppose NorthStar requires technicians to obtain an approval that is routinely unavailable after 5:00 p.m., yet Harbor Point expects emergency support around the clock. Technicians will eventually improvise. The problem is not necessarily technician discipline; the procedure may not match the service reality.

NorthStar should treat repeated workarounds as process signals. If technicians constantly bypass a step, management should ask why. Perhaps the approval model needs an after-hours authority. Perhaps the ticket form requests information the customer cannot reasonably provide. Perhaps the secure file-transfer process is too difficult. Perhaps the standard patch window conflicts with engineering production.

Improvement does not mean weakening security every time someone complains. It means designing controls that can survive real operations. Technicians should be involved in process design because they see where procedures collide with customer reality. Harbor Point should be involved because business constraints belong to the customer. Security personnel ensure that convenience does not erase the intended protection.

A mature program therefore measures not only compliance with procedure but also procedure effectiveness. The question is whether the process produces the intended secure outcome reliably under ordinary and exceptional conditions.

20.60 Root Cause Versus Ticket Closure

Service desks are naturally optimized to close tickets. Security operations sometimes require looking beyond the immediate fix. If a backup fails once because a transient connection dropped, rerunning the job may be sufficient. If the same backup fails every Thursday, closing each ticket independently hides a recurring problem.

The same pattern appears elsewhere. Repeated account lockouts may reveal a stale service credential. Repeated unauthorized software may reveal an unmet business need. Repeated endpoint-agent failures may reveal an incompatible image. Repeated temporary firewall extensions may reveal that the access is no longer truly temporary. Recurrence is information.

NorthStar should therefore have a mechanism for promoting recurring operational events into problem analysis. The objective is not to perform formal root-cause analysis on every minor incident. It is to recognize when repeated symptoms justify deeper investigation and a systemic fix.

This improves evidence as well. A sequence of identical tickets with no analysis suggests that the organization is treating symptoms. A documented corrective action showing that the underlying process was improved demonstrates operational learning.

20.61 Security During Maintenance Windows

Maintenance windows are periods of authorized change, not periods during which security expectations disappear. NorthStar may patch servers, restart services, update network devices, or migrate applications. Monitoring may generate alerts because normal behavior changes. Temporary access may be required. Systems may move through intermediate states.

The change record should therefore identify what is expected during the window and how the team will recognize unexpected behavior. If Beacon receives planned-maintenance information, it can distinguish authorized activity from suspicious activity without blindly suppressing all monitoring. Broad alert suppression may hide an attacker who happens to act during maintenance.

Rollback planning is equally important. A patch that causes an engineering application to fail should have a defined decision path. The team needs to know when to continue troubleshooting, when to restore the previous state, who can make that decision, and how the resulting exception is managed.

After maintenance, NorthStar verifies the intended state. Services running is not always enough. Security agents, logging, backups, application function, and network connectivity may need validation depending on the change. Completion means the environment reached the expected post-change condition.

20.62 Vendor Remote Access

Specialized engineering and manufacturing systems often require vendor support. A vendor may ask Harbor Point to install a remote-access agent or create a permanent firewall rule so its technicians can connect when needed. The request may be operationally convenient, but it creates another administrative path into the environment.

NorthStar and Harbor Point should understand who at the vendor can connect, how authentication works, whether access is always enabled or activated only when needed, what systems can be reached, how sessions are logged, and who approves support activity. A permanent generic vendor account with broad access is difficult to reconcile with accountability and least privilege.

Where practical, access can be time-bound, customer-authorized, restricted to the required system, and monitored. The exact architecture depends on the equipment and vendor capability, but the operating principle remains the same: external support should be an understood path, not an invisible exception created years ago and forgotten.

Periodic review is essential because vendor relationships change. Contracts end, technicians leave the vendor, equipment is replaced, and remote-support technology evolves. Harbor Point should not assume that a remote path remains appropriate simply because it was once approved.

20.63 The MSP’s Supply Chain and Tool Vendors

NorthStar is itself part of Harbor Point’s supply chain, and NorthStar has a supply chain of its own. RMM, PSA, identity, backup, monitoring, documentation, security, and cloud vendors all contribute to NorthStar’s ability to deliver service. A weakness in one provider can affect many customers.

NorthStar therefore needs to understand critical provider dependencies. What service does the vendor perform? What customer information or security protection data does it handle? What administrative capability does it have? What happens if the service is unavailable? How does NorthStar learn about vendor incidents? What alternatives or recovery paths exist?

This does not mean an MSP can eliminate third-party dependency. Modern service delivery depends on providers. The objective is to make dependencies visible and governed. A provider that can execute commands across customer endpoints deserves different scrutiny from a vendor that supplies office furniture.

Chapter 22 will examine the technology stack in greater depth. For Chapter 20, the essential point is operational: NorthStar should know which external services are embedded in its delivery model and how failures or incidents at those providers enter NorthStar’s own response process.

20.64 Business Continuity of the MSP Itself

Harbor Point depends on NorthStar during normal operations and may depend on it even more during an emergency. NorthStar therefore needs to consider how it will continue critical services if its own office, identity platform, Internet connection, RMM, credential system, or primary personnel become unavailable.

A provider continuity plan should focus on the services customers actually depend upon. Can NorthStar receive security escalations if the PSA is unavailable? Can on-call personnel reach emergency contacts? Can privileged access be recovered safely if the primary identity service is disrupted? Can customer documentation be accessed through an approved recovery mechanism? Can NorthStar communicate securely if its ordinary email service is unavailable?

The answers do not need to produce an elaborate disaster scenario for every tool. They should identify critical dependencies and practical recovery paths. A provider that cannot operate during its own incident may leave customers without the support assumed in their security plans.

Testing matters here as well. A recovery credential that has never been exercised, an emergency contact list that has not been updated, or an alternate communication method nobody remembers is only theoretical resilience. Periodic exercises convert assumptions into knowledge.

20.65 Management Review and the Meaning of Continuous Readiness

Continuous readiness does not mean performing an assessment every day. It means maintaining enough operational discipline that the organization does not need a rescue project before every review. Management receives meaningful information, open conditions remain visible, responsibility changes are incorporated, and documentation follows material changes.

Harbor Point leadership does not need to become expert in every NorthStar platform. It does need enough understanding to govern the relationship. Management should know which services NorthStar performs, which responsibilities remain with Harbor Point, which providers matter, what significant exceptions exist, and whether recurring operational reviews indicate deterioration or improvement.

NorthStar leadership has a parallel responsibility. It should understand whether its technicians can follow the processes being promised, whether customer-specific information is current, whether multi-tenant systems preserve separation, whether critical integrations are working, and whether service metrics reveal meaningful exceptions. Leadership should not confuse a favorable dashboard with a healthy operating model.

Continuous readiness is therefore a management condition as much as a technical condition. The organization repeatedly asks whether documented responsibility, actual service delivery, technical state, and available evidence still agree.

20.66 The Operations Playbook as a Training and Quality Tool

Once NorthStar’s playbook is mature, it becomes useful beyond compliance. New technicians can learn how the company expects work to be performed. Team leads can review tickets against a common standard. Quality assurance can identify where procedures are inconsistently applied. Automation designers can see which steps are suitable for automation and which require human judgment.

The playbook also reduces dependence on hero technicians. David may be extraordinarily capable, but an MSP should not require David’s memory to operate

Harbor Point correctly. The playbook captures the stable process while customer documentation captures the environment-specific facts. Expertise remains valuable, but it is supported by organizational knowledge.

Procedures should be written for use, not admiration. A technician facing a failed backup at 2:00 a.m. needs a clear path to triage, escalation, customer communication, and documentation. The detailed rationale can exist in training and reference material, while the operational playbook provides the concise execution path. This separation is why the teaching in this chapter comes before the summary playbook.

NorthStar should periodically observe real use of the playbook. If technicians routinely misunderstand a step, the document may need clarification. If a step no longer matches the technology, it should be updated. A living playbook is part of the operating system, not a static compliance artifact.

20.67 A Contractor's View of a Well-Run MSP Relationship

From Harbor Point's perspective, a mature MSP relationship feels predictable. Requests have known paths. Significant changes do not appear without explanation. Security incidents produce timely, understandable communication. Monthly reviews focus on decisions rather than marketing. NorthStar can explain who has privileged access and can retrieve records without days of confusion. When something fails, the MSP does not hide the exception behind a green dashboard.

Harbor Point also understands its own role. Managers know that access authorization belongs to the business. Employees know which applications and information-sharing methods are approved. Leadership participates in risk decisions that NorthStar cannot make on its behalf. The company keeps its SSP and responsibility understanding aligned with actual service delivery.

This relationship does not eliminate disagreements. Harbor Point may want speed when NorthStar needs more information. NorthStar may recommend replacing a system that Harbor Point considers operationally essential. Beacon may request telemetry that a legacy system cannot provide. Maturity is shown by how those disagreements are resolved: through documented responsibility, risk understanding, technical alternatives, and explicit decisions rather than assumption.

The result is not that Harbor Point becomes dependent on NorthStar for all CMMC knowledge. Instead, the two organizations develop a common operational language.

Harbor Point understands what it is buying and governing; NorthStar understands what it is operating and proving.

20.68 An MSP's View of a Well-Run CMMC Customer

From NorthStar's perspective, a mature customer is not one that says yes to every security recommendation. It is one that participates in decisions. Harbor Point provides timely personnel changes, identifies business owners, communicates new applications and providers, attends governance reviews, and understands that some risk decisions cannot be delegated to the service desk.

A good customer also avoids turning the MSP into an invisible compliance owner. Harbor Point does not say, "NorthStar handles CMMC," and stop there. It asks what NorthStar performs, what evidence NorthStar can provide, what Harbor Point must do, and where responsibilities are shared. That clarity makes NorthStar's service more effective because technicians and managers know where decisions belong.

When Harbor Point disagrees with a recommendation, it explains the operational constraint. NorthStar can then work with the customer to find an alternative rather than treating security as a contest between "yes" and "no." This is particularly important in engineering and manufacturing environments where availability, compatibility, and specialized systems create legitimate constraints.

The strongest relationship is therefore neither customer abdication nor provider domination. It is governed collaboration.

20.69 The Chapter 20 Maturity Progression

An MSP beginning this journey may initially operate reactively. Technicians know customers from memory, privileged access is broad, tickets are brief, exceptions disappear into queues, and evidence is assembled manually. The first improvement is visibility: identify customers, assets, responsibilities, privileged users, critical services, and recurring security processes.

The next stage is consistency. Standard workflows emerge for onboarding, offboarding, change, vulnerability management, backup failures, incident escalation, software approval, and evidence retrieval. Customer-specific overlays preserve necessary differences. Technicians are trained on operational decisions rather than abstract compliance vocabulary alone.

The next stage is integration. Tools exchange information, but integrations are monitored. Expected populations are reconciled. Exceptions have owners. Monthly and quarterly reviews connect technical work to governance. Evidence can be retrieved reproducibly. Provider and customer responsibilities are reflected in service delivery.

The mature stage is not perfection. Failures still occur. Patches still break applications. Backups still fail. Users still request unapproved software. The difference is that the organization detects deviation, responds predictably, learns from recurrence, and preserves enough evidence to explain what happened. Maturity is the ability to operate securely through change and failure, not the absence of change and failure.

20.70 Why This Chapter Matters to the Rest of the Book

Earlier chapters taught scope, responsibility, policy, implementation, evidence, remediation, and assessment. Chapter 20 connects those concepts to daily work. Without this connection, CMMC can remain a parallel compliance program that technicians experience only when someone asks for evidence. With the connection, the requirements become part of identity administration, endpoint management, software governance, vulnerability remediation, recovery, monitoring, incident response, and customer governance.

This chapter also creates the bridge to the next two major operational questions. Chapter 21 asks how NorthStar preserves this discipline when it supports many different defense contractors at the same time. Chapter 22 asks how the technology stack should support those operations without becoming a collection of products purchased for their logos.

The principles developed here will therefore continue to appear: expected populations, customer-specific overlays, responsibility handoffs, provider security, privileged-access lifecycle, evidence from normal operations, exception ownership, and the Random Tuesday test. These are not isolated Chapter 20 concepts. They are the operating vocabulary for the remainder of the book.

The reader should leave this chapter with a practical standard: if a security process exists only in a policy, it is not yet operational; if it exists only in a technician’s memory, it is not yet resilient; if it creates no reliable record, it will be difficult to demonstrate; and if it works only during assessment preparation, it is not yet continuous readiness.

20.71 The Random Tuesday Test

NorthStar's final operational exercise is deliberately simple. The service manager chooses an ordinary Tuesday from six months earlier without giving the team advance notice. The team reconstructs the important security operations for Harbor Point using normal records. Who had privileged access? Which endpoints were expected? Which were reporting? Which vulnerabilities were open? Which backups failed? Which changes occurred? Which security events required action? Which exceptions existed?

The purpose is not to reconstruct every keystroke. The purpose is to discover whether NorthStar can explain the security-relevant operation of Harbor Point using reliable organizational records rather than personal memory. Where the answer is difficult, NorthStar has identified an improvement opportunity: missing documentation, weak integration, unclear ownership, incomplete retention, or a process that exists more strongly on paper than in practice.

20.72 The Final Operational Test

At the end of Chapter 20, the strongest question remains the one with which this final expansion began: if everyone stopped talking about CMMC tomorrow morning, would these security processes continue? Would onboarding still begin with authorization? Would privilege still follow responsibility? Would missing endpoints still be investigated? Would software still move through approval and lifecycle management? Would failed backups still be examined? Would incidents still follow defined escalation? Would exceptions still have owners? Would quarterly reviews still challenge assumptions?

If the answer is yes, the organization has moved beyond assessment preparation. CMMC has become part of the operating model. If the answer is no, the weakness is useful information. It shows where the organization still depends on assessment pressure rather than sustainable process.

20.73 Chapter Conclusion

Building CMMC into MSP operations does not mean turning every technician into a CMMC assessor. It does not mean attaching a compliance checklist to every ticket. It means translating security expectations into repeatable operational behavior. The customer authorizes. The MSP implements the services it owns. Shared activities have defined handoffs. External providers understand their roles. Privileged access

follows job responsibility. Devices, software, and services enter and leave deliberately. Changes are understood. Vulnerabilities move toward resolution. Backups are tested through recovery. Security events move through defined escalation. Exceptions remain visible. Documentation follows reality. Evidence emerges from the work.

The strongest MSP operating model is not the one that produces the largest compliance binder. It is the one in which an ordinary Tuesday produces enough reliable operational evidence to explain how the environment was protected. That is the standard NorthStar has been building with Harbor Point.

Normal operations should create security. Normal operations should create evidence. Normal operations should maintain readiness.

Transition to Chapter 21 - Managing Multiple CMMC Customers

We have intentionally spent a great deal of time with one customer because Harbor Point allowed us to slow the operating model down and see how the pieces connect. NorthStar, however, is an MSP. It may support ten defense contractors, fifty, or hundreds. Those customers will not share identical architectures, providers, CUI flows, technologies, contracts, or internal capabilities.

The very systems that allow NorthStar to scale - multi-tenant RMM, PSA, credential, documentation, automation, and monitoring platforms - can also create new risks. Maria may support several CMMC customers in the same day. Automation may reach many environments. A report may expose another customer. One customer’s emergency authority may not apply to another. A standard security baseline may need customer-specific overlays.

Chapter 21 therefore changes the question. We are no longer asking only whether NorthStar can operate Harbor Point securely. We will ask whether NorthStar can operate many different CMMC customer environments securely, consistently, and at scale without losing customer separation, responsibility clarity, evidence quality, or control of technician access.

Operational Reference: Chapter 20 Playbook Summary

The following reference is intentionally placed after the teaching. It is not a substitute for the explanations in this chapter. It is a compact operational map that NorthStar

could use to ensure that recurring processes have clear triggers, ownership, records, exception paths, and completion criteria.

Operational Process	**Typical Trigger**	**Completion Condition**
Customer onboarding	Authorized sales/project handoff and discovery	Known environment, responsibilities, open risks, transition to steady state
Technician onboarding	Approved customer assignment	Required access provisioned and verified; no unnecessary privilege
User onboarding	Authorized customer request	Identity, role access, endpoint and protections validated
User role change/offboarding	Authorized personnel event	Access adjusted or removed across relevant systems and verified
Endpoint lifecycle	New, reassigned, repaired, or retired device	Asset state, management, security coverage and disposition verified
Software/service request	Business request or discovery of new application	Approved/rejected decision, controlled deployment, inventory and lifecycle ownership
Privileged access	Approved administrative need	Specific privilege granted, reviewed, and removed when no longer required
Change management	Proposed technical change	Authorized, implemented, validated, documented; rollback/exception handled
Vulnerability management	Validated finding	Risk addressed, exception owned if needed, remediation verified
Patching	Approved update cycle or urgent patch	Expected population reaches target state or exceptions are owned
Backup/recovery	Scheduled job, failure, or test	Protected workload backed up; recovery capability periodically validated
Logging/SOC	Expected telemetry and detection service	Coverage reconciled; meaningful events investigated and escalated
Incident response	Event meets escalation criteria	Containment, investigation, recovery, communication and lessons completed
Evidence retrieval	Governance or assessment request	Customer-specific authoritative records retrieved reproducibly
Monthly review	Recurring governance cadence	Meaningful conditions, decisions

		and owners recorded
Quarterly review	Recurring deeper review	Scope, providers, access, architecture, exceptions and documentation challenged
MSP platform change	Material provider technology change	Security impact understood; migration and customer implications controlled
Customer offboarding	Authorized termination/transition	Access, agents, data, credentials, monitoring and responsibility transitioned securely

Source Notes

[1] U.S. Department of Defense Chief Information Officer, CMMC Assessment Guide - Level 2, Version 2.13. See CM.L2-3.4.8 (application execution policy) and CM.L2-3.4.9 (control and monitoring of user-installed software). Official resource: https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL2v2.pdf

[2] U.S. Department of Defense Chief Information Officer, CMMC Assessment Scope - Level 2, Version 2.13. See guidance on significant architectural or boundary changes and External Service Provider considerations, including SSP documentation and customer responsibility matrices. Official resource: https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2v2.pdf

Publication note: CMMC implementation status and official guidance can change. Regulatory-status statements should be reverified against the official DoD CIO CMMC resources immediately before final book publication.

CMMC for MSPs

From Readiness to Certification

Chapter 21

Implementing and Maintaining CMMC Across Three Parties

Authored by Dr. Charles Edwards

Final Teaching Edition

Chapter contents by section

21.1 From a purchased solution to an operating security program

21.2 Party ABC and the independent assessment function

21.3 Party EGH and the implementation function

21.4 Party IJK and continuing accountability

21.5 Understanding the information before selecting the technology

21.6 Organizing the work into three phases

21.7 GCC and GCC High in plain language

21.8 Deciding between the cloud environments

21.9 Building a software and license register

21.10 Collaboration subscriptions and the underlying platform

21.11 Identity protection and privileged access

21.12 Endpoint management and operating system rights

21.13 Endpoint detection and response

21.14 Email protection and information protection

21.15 Audit logs and security monitoring

21.16 Vulnerability management and patching

21.17 Backup and recovery services

Chapter contents by section continued

21.18 Remote administration and supporting tools

21.19 Who owns the tenant and who owns the software

21.20 How long each party remains responsible

21.21 Implementing the selected environment step by step

21.22 Testing and accepting the implementation

21.23 Transferring knowledge and limiting installer access

21.24 Daily and weekly maintenance

21.25 Monthly quarterly and annual maintenance

21.26 Internal reporting and management decisions

21.27 CMMC status and affirmation reporting

21.28 Cyber incident reporting and evidence preservation

21.29 Evidence that remains useful after installation

21.30 Managing changes and provider transitions

21.31 A worked example of the first operating month

21.32 Bringing the responsibilities together

Chapter reference tables

Sources and further reading

21.1 From a purchased solution to an operating security program

An organization does not become ready for a Cybersecurity Maturity Model Certification assessment simply because a contractor installs security software. It becomes ready when its people, processes, technologies, and records work together within a clearly defined assessment scope. The same organization must then keep those protections functioning while employees change, subscriptions renew, equipment fails, customers introduce new requirements, and attackers look for weaknesses. This chapter explains how to organize that work when different companies perform the assessment, installation, and ongoing maintenance.

We will follow three fictional parties throughout the discussion. Party ABC provides independent assessment services when properly authorized for the assessment being purchased. Party EGH designs and implements the technical environment. Party IJK operates and maintains the environment after handover. In our main example, IJK is an MSP preparing its own organization for an applicable CMMC assessment while also developing the capability to support defense contractor customers. These roles are illustrative. They do not establish the credentials, contracts, or assessment independence of any actual company.

The central lesson is that responsibility must survive every handoff. An installer can enable an audit setting, but someone must verify that the resulting records continue to arrive. An assessment organization can examine evidence, but management must keep the underlying practice operating afterward. An MSP can maintain another company's environment, but the customer still needs accountable leadership, authorized decisions, and an accurate understanding of the obligations attached to its contracts.

Our approach is deliberately practical. We will begin with the people and business interests involved, then examine the information being protected, the choice between Microsoft government cloud environments, the software and licensing needed to implement the design, and the operating procedures that keep it reliable. We will also examine reporting, evidence preservation, subscription ownership, incident response, and provider transition. The goal is to help the reader understand why each activity exists and how to perform it in an organized way.

The implementation schedules, staffing patterns, and internal review frequencies in this chapter are examples for planning. They are not universal CMMC deadlines. Contract clauses, assessment requirements, license terms, and documented

organizational policies determine the obligations that apply to a particular organization. Product names identify possible implementations of a capability; they do not constitute a required shopping list or a promise that purchasing those products produces certification.

21.2 Party ABC and the independent assessment function

What ABC actually examines and why independence matters

In the Harbor Point example, ABC's first question is not which license Harbor Point purchased. It is what entity seeks the assessment, which contract requires the status, what systems form the assessment scope, and which external providers operate or protect those systems. A precise engagement letter identifies the assessed organization, the planned level and assessment path, the environment to be assessed, assessment dates, authorized personnel, evidence handling, and permitted follow-up. If Harbor Point seeks a C3PAO assessment, ABC's current authorization and the applicable impartiality requirements must be checked through authoritative program channels before the engagement is accepted. ABC's name on a sales presentation does not establish those facts.

ABC needs to examine whether the documented system and the operating system match. The system security plan might say that IJK revokes a departing employee's account within the approved process. ABC could examine the procedure, interview the manager who notifies IJK, review selected termination records, and test how the organization locates the relevant account and device evidence. It may ask about an exception. Harbor Point and IJK should answer from their actual records, including failures and corrections. EGH can explain the configuration it delivered, but an installer cannot supply six months of routine operating history merely by recreating screenshots during assessment week.

ABC's independence shapes communications before and during the assessment. IJK can ask logistical questions about the process and evidence format, while ABC can identify the assessment objectives and request clarifying evidence. ABC should not become the architect of Harbor Point's controls, choose the customer's software on its behalf, direct EGH's remediation, and then assess the result as though its own work were independent. The parties should document any prior advisory relationship and determine the permissible arrangement under current program requirements. Where necessary, Harbor Point can obtain separate readiness consulting and reserve ABC for the independent assessment.

Assessment fees and terms deserve the same precision as technical procurement. The agreement should identify the assessment scope and assumptions, expected interviews and demonstrations, travel or remote logistics, secure evidence exchange, handling of sensitive material, report delivery, schedule changes, and authorized closeout work. It should explain what additional work costs and who may approve it. Harbor Point should not buy an undefined promise that it will pass; ABC's legitimate product is an independent assessment performed under the applicable process. Its obligation ends according to that engagement and program duties, not when Harbor Point no longer needs security management.

Party ABC is a fictional organization whose background is in cybersecurity assessment, evidence evaluation, and the examination of security requirements. Where a contract requires a Level 2 third-party certification assessment, the assessment organization must possess the appropriate authorization as a CMMC Third-Party Assessment Organization, commonly called a C3PAO. A consultant with cybersecurity experience, a security certification, or a partnership with a software manufacturer is not automatically a C3PAO. IJK must verify the specific organization's current authorization and the assessment services it is actually qualified to perform.

ABC's business interest is to deliver a defensible assessment through a process that preserves independence and evaluates the defined scope fairly. Its assessors need access to relevant personnel, system configurations, written procedures, and operating evidence. They must be able to distinguish between a policy that describes an intended practice and records showing that the practice is implemented. An attractive dashboard, a vendor certificate, or a folder full of templates cannot substitute for an examination of the organization's own implementation.

The engagement must separate readiness advice from independent certification work. A readiness review can help an organization understand gaps, but consulting and assessment relationships must be checked against applicable impartiality and conflict-of-interest requirements. IJK should not assume that ABC may design the controls, implement them, coach every answer, and then independently assess its own work. When the proposed arrangement creates an independence concern, IJK should obtain readiness support from a separate provider and preserve the assessor's independent role.

Consider a question about access reviews. ABC may ask how IJK decides that an employee still needs access to a controlled project workspace. EGH can demonstrate

the groups and permissions it configured, but IJK must explain who approves membership, how changes are recorded, and how inappropriate access is removed. ABC evaluates the resulting evidence. It does not become the continuing owner of IJK's access approval process merely because an assessor examined that process.

ABC's period of responsibility follows its assessment agreement and applicable program obligations. The agreement should identify preparation activities, assessment dates, evidence handling, permitted follow-up, any authorized closeout work, report delivery, and record retention. A completed assessment does not create an unlimited maintenance contract. If IJK wants additional advisory services later, those services require an appropriate engagement and another independence review where necessary.

21.3 Party EGH and the implementation function

EGH as architect, installer, and temporary custodian

EGH starts with an approved design basis. Harbor Point provides contractual and data-handling requirements; IJK supplies the existing asset inventory, network dependencies, privileged paths, and support processes. EGH produces a design that names each service, its location, the information it handles, who administers it, and how its operation will be tested. Design approval should belong to Harbor Point's authorized leaders, with IJK confirming that the design can be maintained. When a consultant's proposed configuration cannot be supported by the people who will operate it, the gap should be resolved before procurement rather than handed to the help desk as a permanent exception.

The statement of work should identify which parts EGH will install and which parts it will only recommend. For a government tenant it might include eligibility and purchasing coordination, identity foundation, pilot accounts, device enrollment, mail and file migration, baseline policies, security integrations, testing, and handover. It should state whether EGH will migrate historical mail, audit records, Teams content, third-party application integrations, and device profiles. An item omitted from the scope should not silently be assumed complete because the new tenant accepts sign-ins. Conversely, new work requested during installation should pass through documented change control rather than altering the contract by casual conversation.

EGH's privileged access is a temporary operational necessity with a measurable end. It should use individual identities and approved authentication, record changes, avoid unowned shared accounts, and place scripts and configuration exports in Harbor

Point-controlled repositories. During stabilization, it may retain narrow access for defined defects. At closure, IJK and Harbor Point review user and application permissions, delegated administration, certificates, tokens, remote agents, and support relationships. They revoke or transfer each item deliberately, then test that normal operations still work. The end of EGH's invoice does not automatically revoke a service principal or disable a migration agent.

A two-month stabilization period can be appropriate in the example, but it is a contract choice rather than a CMMC rule. The agreement should identify its start trigger, covered defects, response and escalation times, exclusions, final acceptance, and data return or deletion obligations. IJK should take the lead during stabilization so that EGH becomes a backstop rather than the only person who knows the environment. If Harbor Point later wants EGH to perform continuous engineering, that is a new service relationship with its own scope, evidence obligations, and access review.

Party EGH is a fictional systems integration company with practical experience in identity, endpoint management, cloud migration, logging, network security, and backup. It translates approved requirements into technical settings and repeatable procedures. Its engineers may establish a tenant, configure authentication policies, enroll devices, deploy endpoint protection, connect logs, build backup jobs, and document the resulting environment. The organization should evaluate these capabilities directly rather than relying only on an attractive product proposal.

EGH's business interest is to deliver the contracted implementation successfully, earn the agreed project revenue, and possibly provide an explicitly defined stabilization or support service. These interests are legitimate, but they create decisions that IJK must manage. A reseller may prefer a familiar license bundle. An engineer may favor a product that is easier to deploy. IJK must ensure that the final design satisfies its information protection needs, staffing capacity, and long-term operating budget.

A useful implementation statement of work describes deliverables in terms that IJK can test. The phrase install endpoint protection is incomplete. A stronger deliverable identifies the covered devices, the approved configuration, the reporting destination, the administrator roles, the alert routing, the test method, and the evidence to be supplied. Similarly, configure backups should identify the protected workloads, restore procedures, storage boundaries, access controls, recovery objectives, and acceptance tests.

EGH should not be allowed to make material scope decisions silently. If the company discovers a production workstation that cannot support the planned security agent, it must document the issue and seek an approved treatment. Possible responses include replacement, an appropriately designed isolation approach, or revision of the operating process. Simply excluding the workstation from the dashboard does not remove it from the assessment scope if it still handles relevant information.

The implementation relationship should have a clear end point. A project may include a defined period for defect correction and stabilization, but that period should have an actual start date, end date, escalation path, and description of covered work. Routine administration after that period belongs to IJK or to a separately contracted operator. A statement that EGH will help when needed is too vague to support a security program.

21.4 Party IJK and continuing accountability

Two accountable leaders and an operating team

IJK's leadership needs a written allocation that survives vacation, illness, and employee turnover. One leader can own contracts, subscriptions, customer commitments, the evidence calendar, and management review. Another can own technical standards, privileged administration, tool health, incident coordination, and recovery. Their responsibilities overlap at important decision points. A license cancellation can disable a control; a technical change can create a new contractual data flow. The leaders therefore need a recurring review of decisions and an alternate for each critical action, while retaining separate approval and execution where practicable.

A technician's role should be defined by procedure and access, not by a vague instruction to keep the environment secure. The onboarding technician verifies an approved request, issues a managed device, assigns the correct identity and license, enrolls the device, confirms endpoint protection and backup where applicable, and closes the ticket with evidence. A second technician or manager may review privileged changes. The offboarding procedure receives an authoritative trigger, disables access, revokes sessions and tokens, recovers equipment, addresses shared secrets, and checks external applications. Each task has a timestamp, owner, and exception route. The process is designed so an unfamiliar qualified employee can perform it from the record.

For customer services, IJK must separate its own protected environment from each customer's assessment scope. Harbor Point's customer-owned tenant, backups, and tickets may generate different responsibilities from those in IJK's internal tenant. IJK should maintain a customer-specific service description and responsibility matrix: what it administers, which data it sees, which controls depend on its service, what evidence it produces, who receives alerts, and when it must notify the customer. A single generic promise to support CMMC can conceal a gap between the customer's expectation and the MSP's actual service catalog.

Continuity also means financial and organizational capacity. If only one engineer understands a backup key, the backup may be technically sound but operationally fragile. If the company stops paying for a log service at renewal, its documented monitoring process can fail. IJK should budget for licenses, labor, training, alternate coverage, periodic recovery exercises, and outside specialist assistance when appropriate. Management needs to recognize that its obligation continues while its own applicable contracts and customer service agreements continue, and that termination requires an orderly transfer of service and information.

Party IJK is a fictional MSP with a small leadership team and a limited number of technical employees. In the main example, two senior leaders share responsibility for maintaining the company's protected environment. One concentrates on administrative governance, contracts, renewals, and evidence coordination. The other concentrates on technical operations, configuration review, incident handling, and recovery. This arrangement can work, but the two people need documented responsibilities, backup coverage, and a method of reviewing each other's privileged actions.

IJK has several interests in CMMC. It may need an applicable status to compete for or perform covered work. It wants to protect its own sensitive business and customer information. It also wants to provide credible services to customers that face defense supply chain requirements. These interests should not be confused. An MSP's successful assessment does not automatically confer the same status on every customer, and the fact that a customer is assessed does not automatically settle the MSP's own scope or external service provider obligations.

IJK's management owns the decisions that no vendor can make on its behalf without authorization. These include approving the assessment boundary, allocating the operating budget, authorizing access, accepting implementation deliverables, and ensuring that required affirmations are supported. An engineer can explain the risk of

a proposed exception, but management must decide how the organization will resolve it within applicable requirements. A signed risk acceptance does not waive a contractual or assessment requirement.

In a customer engagement, the customer becomes the organization seeking assessment for its own scope, while IJK may act as an external service provider. The customer should appoint its own accountable official and business owners. IJK should identify which services it performs, what information those services handle, what security protection functions they provide, and what evidence the customer can obtain. A service description that merely promises CMMC support does not establish those responsibilities.

IJK's maintenance obligation continues for the period established by its own obligations and, where it serves a customer, its service contract. It does not end on assessment day or automatically after the implementation warranty expires. If a contract requires a current CMMC status throughout performance, operations must support that continuing requirement. The company should plan for absences, departures, and emergencies so that the program does not depend on one person's memory or personal account. [1]

A complete three-party engagement

Before Party ABC accepts an assessment assignment, it needs to know the entity and system that will actually be assessed. Party IJK may be a managed service provider with its own protected environment, while its customer may be a manufacturer whose engineering team receives controlled drawings. These are two organizations with different contracts and potentially different assessment scopes. ABC should confirm the assessment applicant, level, assessment type, boundaries, external service providers, and independence conditions in its engagement. A statement that ABC will assess the whole relationship is too imprecise to determine whose requirements are being examined.

Party EGH enters the relationship as an implementer. Its interest is a project with a defined design, deliverables, acceptance tests, and payment milestones. To plan that work, EGH may need access to diagrams, user and device inventories, existing configurations, and contract-derived requirements. It does not acquire authority to redefine the customer's protected information or declare an unfavorable system out of scope. When its engineering discovery conflicts with the customer's original assumptions, EGH should document the conflict, identify the technical options,

estimate effects on cost and schedule, and return the decision to IJK's authorized leadership.

Party IJK's interest continues after the installer and assessor have left. If IJK is protecting its own environment, its leaders approve the boundary and budget, operate the controls, maintain evidence, and support affirmations where applicable. If IJK manages a customer environment, the customer retains its contractual and organizational decisions while IJK performs precisely described services. This distinction should appear in the service agreement and the system security plan. A customer cannot transfer an affirming official's judgment to a help desk simply by purchasing managed security services.

Suppose the parties begin in January with a planned implementation in March and an assessment in September. ABC's independent assessment engagement may occupy the defined assessment period and permitted follow-up; EGH's installation statement of work may end after acceptance and a sixty-day stabilization period; IJK's operation may continue under a renewable customer agreement and through its own applicable contracts. Those dates are hypothetical planning choices. Each real agreement needs its own start, end, renewal, termination, record-retention, and transition provisions. An expired implementation warranty must never become the reason an essential security function stops working.

21.5 Understanding the information before selecting the technology

Tracing a drawing through a normal workday

Harbor Point's program manager receives a drawing from a prime contractor through a designated portal. The drawing has a project identifier, revision number, and markings that the company must interpret in the context of the contract and the originator's directions. The program manager forwards a notice to the engineering lead, who downloads the drawing to a managed workstation, places the current revision in the approved project repository, and asks two engineers to review it. This ordinary sequence already involves the portal, the manager's identity, browser and device, local download path, repository, engineers' endpoints, and the notification channel. If one engineer later attaches a screenshot to a support ticket, another system enters the information flow. The first design exercise is to trace the real path, not to list the ideal tools on a purchase order.

The data owner and contract lead determine what the material is and what handling obligations apply. IJK helps discover every technology that receives or protects it,

while EGH maps how the proposed architecture changes those paths. Neither provider should decide classification from a filename alone. The drawing may have older revisions and derivative material: comments, extracted dimensions, printouts, meeting recordings, search indexes, and backup copies. A workflow interview should ask where each is created, how long it persists, who can retrieve it, and how it leaves the organization. The result may change the planned scope more than a scan of the central file repository does.

A useful map includes people as well as systems. The prime's contact sends the drawing; Harbor Point's program manager accepts it; engineers work with it; a quality reviewer may approve a change; IJK technicians may see the desktop during support; EGH engineers may have access while migrating files; and the backup provider may hold an encrypted copy. The map should identify the purpose of each access and the authority that grants it. A general administrator is not automatically entitled to inspect project content simply because the platform technically permits it. Conversely, an administrator who can change security settings may be relevant to scope even when the administrator never opens the drawing.

The team then tests an ordinary exception. An engineer traveling to a customer's site wants to review the drawing offline. Does the approved device retain an encrypted local copy? Can it synchronize when reconnected? Does the engineer need to print? Who approves a transfer to the customer, and through which service? The answers may require changes to device management, sharing policy, and the employee procedure. A design that works only when everyone sits at one desk is unlikely to survive operations. Harbor Point should approve the actual permitted behavior, EGH should configure and test it, and IJK should maintain the resulting controls and evidence.

The map becomes a living design input. A later decision to use a CAD collaboration platform, external review service, or automated classification tool can create a new data path even if the main GCC High tenant remains unchanged. IJK's change request should refer back to the map, describe the new service and provider commitments, and identify whether the system security plan, licenses, backup, logs, and incident contacts change. Harbor Point's data and contract owners decide whether the new path is allowed. This process gives the organization a way to adapt without pretending that the original diagram remains accurate forever.

Before the parties discuss products, they must understand the information involved. Federal Contract Information, or FCI, and Controlled Unclassified Information, or

CUI, are different categories with different consequences for the applicable assessment and safeguards. Information is not CUI merely because an MSP considers it confidential. Conversely, the absence of a convenient label does not justify ignoring contractual instructions or information that requires clarification from the customer or contracting authority.

IJK should begin by examining contracts, customer instructions, project workflows, and the places where information enters its environment. An employee may receive technical information by email, save a copy in a project folder, open it on a laptop, print part of it, and send a support ticket containing a screenshot. Each step changes where the information resides and who can access it. A scope discussion that considers only the original mailbox misses the rest of the workflow.

For our example, assume IJK has twenty-four employees, but only eight require access to a controlled engineering support project. The company also has two technical administrators, shared business services, and several outside suppliers. These numbers are planning assumptions, not licensing rules. The parties must determine whether a separate controlled environment is practical, which administrative systems can affect it, and how information will be prevented from moving into ordinary business tools.

An enclave is a deliberately bounded environment used for a particular protected workload. It may reduce the number of users and systems directly handling CUI, but it is not created merely by naming a folder restricted. The architecture must address identity, endpoints, administrative access, file movement, printing, backups, remote sessions, and security tools. The evidence must support the claimed boundary under the applicable assessment scoping guidance.

The scope also includes the relationships around the technology. An outside help desk may see sensitive filenames, a monitoring provider may collect security protection data, and an installer may use privileged remote access. These relationships require analysis even when the provider says it does not routinely open customer documents. IJK should document the actual data and security functions involved, then apply the current external service provider and cloud service provider rules to those facts.

A customer case that makes the roles concrete

Imagine that Harbor Point Engineering is a twenty-four-person subcontractor receiving controlled technical drawings from a prime. Eight engineers need regular

access to that material, two managers approve project membership, and a small accounting team does not ordinarily use the controlled workspace. Party IJK is Harbor Point's MSP and administers identity, endpoints, backup, and remote support. Party EGH has been retained for a government-cloud migration. Party ABC is being considered for a later independent assessment, assuming its authorization and impartiality are confirmed. Harbor Point itself is the contractor with the relevant contract; it cannot disappear from the responsibility model merely because three providers have been named.

At the first discovery meeting, Harbor Point's program manager identifies the specific contract and prime-contractor flowdown, while its data owner identifies the drawing types and how they are received. IJK brings a current list of managed users, devices, support tools, privileged accounts, and third-party platforms. EGH asks where the drawings go when an engineer opens them, prints them, attaches them to a ticket, or synchronizes them to a laptop. ABC, if consulted only for permissible preliminary logistics, would need to avoid becoming the designer of the system it will independently assess. The outcome of discovery is a shared factual record, with disputed assumptions assigned to a named owner for resolution.

The scope map may reveal that the eight engineers are only part of the affected environment. A general-purpose help desk platform could receive screenshots of drawings. An RMM platform can run code on their laptops. A backup platform copies their files. Identity administrators can grant access to the workspace. Each connection needs a documented treatment: include the asset, redesign its access or data flow, establish isolation, or provide a justified exclusion under the applicable scoping rules. EGH may recommend the technical treatment, IJK may implement ongoing controls, and Harbor Point approves the business architecture and documentation.

Only after that analysis does Harbor Point authorize a purchase. Suppose it chooses GCC High for the controlled workspace based on its information, contract analysis, service commitments, and interoperability tests. EGH builds the tenant and migration plan; IJK prepares its operating processes and support agreements; Harbor Point retains legal control of the tenant and receives administrative and billing visibility. ABC later examines the defined system and supporting evidence through its independent assessment engagement. The example illustrates why buying licenses at the first meeting would have put an uncertain product choice ahead of the information flow.

21.6 Organizing the work into three phases

A decision record that survives the project team

The first phase should end with an approved design basis. Harbor Point's leadership records the contractual requirement being addressed, its information-flow map, the intended assessment boundary, the roles of ABC, EGH, and IJK, and material assumptions requiring confirmation. The record should name the person authorized to decide each issue. For example, the contract lead decides whether a prime flowdown applies; the data owner decides which business process needs access; EGH explains whether a proposed integration is technically supported; IJK explains whether it can operate and monitor it; and Harbor Point's management approves the expenditure and remaining risks within applicable requirements. The record should make disagreements visible rather than erasing them from the final diagram.

The second phase turns that approved basis into a testable implementation. EGH creates a build sequence and a configuration baseline, including identity, device, application, network, logging, backup, and support paths. It identifies dependencies: a conditional access policy should not be enforced before pilot devices are enrolled, and a migration should not remove the source repository before backups and retention have been checked. Each task has a completion test and a rollback or recovery approach. IJK participates throughout, because an operator who first sees the system at the final handover cannot easily distinguish an intentional design choice from a temporary installer workaround.

The third phase is acceptance and sustained operation. IJK repeats representative tasks using the runbooks, Harbor Point reviews the business outcomes, and EGH closes documented defects. An accepted installation is a starting configuration, not a history of continuous operation. Over subsequent weeks IJK produces ordinary access, monitoring, patch, restore, and change records. Harbor Point's management reviews exceptions and funds the necessary service. ABC, if later engaged for an independent assessment, examines the scope and implementation under the applicable assessment process. The three phases overlap at their boundaries, but the decision rights should remain clear.

Consider a change request halfway through the build. Harbor Point discovers a legacy application that must send project notices through email. EGH proposes an application identity and mail permission; IJK notes that the proposed permission is broad and that the application lacks an owner. The project team records the business

need, data content, required permission, alternatives, license effects, monitoring, and shutdown procedure. Harbor Point approves a bounded design or delays the feature. This is more useful than quietly granting a high-privilege application permission so that the migration schedule appears green.

The decision record should be handed to future operators alongside configurations. Months later, an administrator may ask why external sharing is limited, why one device group has a different policy, or why a service account is excluded from an interactive login rule. A dated rationale, approval, and test result allow the team to distinguish a deliberate exception from drift. The record should also identify review triggers such as a new contract, provider, application, data category, or work location. It need not be a large bureaucracy; it must be sufficient to preserve the reasons behind important choices.

The first phase is readiness and design. IJK establishes the business need, identifies applicable obligations, defines the proposed scope, and evaluates gaps. EGH contributes technical feasibility and implementation estimates. ABC participates only within an appropriate independent assessment role or other permissible engagement. The principal output is an approved plan showing what must change, who will implement it, how success will be demonstrated, and how IJK will sustain it afterward.

The second phase is implementation and controlled handover. EGH configures the approved environment, tests representative workflows, corrects defects, and transfers operational knowledge to IJK. IJK supplies business decisions, participates in testing, and learns the procedures before accepting the work. The parties should treat handover as a series of demonstrated capabilities, including account recovery and evidence retrieval, rather than a single meeting followed by a collection of passwords.

The third phase is sustained operation and assessment support. IJK runs the program, maintains evidence, corrects failures, manages change, and prepares the organization for the applicable assessment activities. An independent assessment is scheduled when the implementation and operating evidence justify it. A three-phase business model does not mean all assessment-related work happens before installation or that maintenance waits until certification. Operational evidence begins accumulating as the environment becomes functional.

For planning, IJK might allocate several weeks to discovery, several more to staged implementation, and a stabilization period before an independent readiness decision. These durations depend on the starting condition, migration complexity, staff

availability, and assessment scheduling. A business deadline should not be converted into an unsupported promise that every control will be implemented by a fixed date. The plan should identify dependencies and explain what would require a schedule adjustment.

At each phase transition, IJK should record a decision. The design approval accepts the proposed scope and resources. The implementation acceptance confirms that specified deliverables passed their tests and that remaining work is understood. The readiness decision confirms that management has sufficient evidence to proceed. These decisions create accountability without transferring the assessor's judgment to the installer or confusing project completion with certification.

21.7 GCC and GCC High in plain language

The tenant boundary and its connected services

When Harbor Point considers GCC High, it should distinguish the Microsoft service boundary from its own complete system. The tenant contains identities, mail and collaboration services, policies, and administrative roles. Engineers also use laptops, a CAD application, a backup service, a ticket portal, an RMM agent, and sometimes an external customer portal. Each connection has its own information flow and provider role. A document stored in a government tenant can leave that boundary when an employee sends it through an unapproved attachment, a support agent captures a screen, or a third-party integration copies it. The architectural review should show those exits and decide whether to block, redesign, or govern them.

Service availability differs between environments and changes over time. EGH should maintain a feature validation worksheet for the exact proposed plan and government cloud. A row records the feature, why it is required, vendor service documentation, license dependency, government-environment availability, pilot result, and owner who accepted the result. The worksheet might cover external sharing, mobile application management, retention, data loss prevention, endpoint detection, audit export, and a specific third-party connector. If a feature is unavailable, the team should choose a supported method and test it rather than implying that the commercial demonstration proves the government version works. [3, 4]

Eligibility and procurement should be handled early. Harbor Point supplies the organizational information necessary to establish that it qualifies for the intended government offering. The authorized purchaser verifies the reseller and purchase

terms. EGH may coordinate setup, but the tenant should be created under the correct legal entity with company-controlled recovery and billing contacts. A project engineer's personal account or a reseller-only administrative identity should not become the sole route back into the company's service. IJK should receive appropriately scoped administration during build and verify that authorized Harbor Point personnel retain organizational control.

A higher-priced environment should have a clear business rationale. If the approved workload needs particular provider commitments or collaboration boundaries, leadership can compare the cost of GCC High with alternatives that genuinely meet the same requirements. The comparison includes migration expense, user training, application compatibility, recurring licenses, help desk burden, backup and log services, external partners, and future provider transition. A cheaper primary subscription may require additional controls or services; an expensive subscription does not eliminate operational labor. The decision is strongest when it records the actual obligations, capabilities, and costs rather than a claim that one label is universally required.

The boundary should be revisited when the organization adds services. A new AI assistant, transcription service, digital signature system, backup product, or support portal can process content or security protection data. Even a feature inside the tenant may introduce a new setting, licensing term, or data behavior. Harbor Point should require a small architectural review before activation, including a test account and sample non-sensitive data when feasible. IJK updates the inventory and monitoring plan, and EGH participates only if an active engineering agreement assigns it that work. The service environment remains a deliberate choice rather than a one-time label.

What the government tenant changes and what it leaves to the customer

A tenant is an administrative boundary for identities, policies, subscriptions, mail, files, and collaboration services. Selecting GCC or GCC High establishes where a particular Microsoft government service is delivered and which service commitments and features may be available. It does not determine the customer's contract clause, classify every document, or configure every control. Harbor Point must still decide what information belongs in the protected workflow and who may reach it. IJK must still operate the tenant, manage devices and administrator access, review logs, and respond to failures. EGH must still prove that the approved design works before handover.

The comparison should be made service by service. The team should ask whether the exact mail, document, identity, endpoint, security, and integration services needed are offered in the chosen environment and on the proposed plans. It should identify external collaboration partners and test their ability to communicate and exchange information under the chosen settings. Government service descriptions note feature and boundary differences; a demonstration in a commercial tenant is not sufficient evidence for a GCC High deployment. Eligibility, purchase route, support arrangements, and actual provider commitments should be confirmed in current Microsoft materials and the purchase agreement. [3, 4]

Harbor Point's choice may be shaped by contractual requirements that extend beyond a generic CMMC level. Covered defense information in an external cloud can bring the specific DFARS 252.204-7012 cloud requirements into view. Export-control restrictions, prime-contractor terms, customer expectations, or an approved alternative architecture may also matter. The contractor should get the relevant interpretation from appropriate contractual and professional authorities. EGH can show technical consequences of each option, but should not turn a marketing claim into a legal determination. The written decision should distinguish confirmed obligations from assumptions awaiting resolution. [2]

The real benefit of an appropriate environment is the ability to use a service whose documented commitments fit the approved information flow while retaining familiar collaboration capabilities. The benefit has limits. A misaddressed message, overly broad SharePoint permission, unmanaged personal laptop, uncontrolled support attachment, or missing administrator review can still expose information. Harbor Point should describe the exact tenant and connected systems in its scope documents and test ordinary business behavior after deployment. The service environment supports the program; it is not the program.

Microsoft's Government Community Cloud is commonly called GCC. GCC High is a separate government cloud offering with a different architecture and service commitments. The correct name is GCC High, rather than High GCC. A tenant is the organization's logical service environment in which accounts, subscriptions, policies, and collaboration resources are managed. Choosing the tenant environment is therefore an architectural and contractual decision, not simply a selection of a higher-priced email package.

Microsoft describes GCC as a government offering for eligible organizations and GCC High as an offering intended for eligible organizations with relevant defense

and export-controlled information needs. Its service descriptions also identify differences in the surrounding cloud environment, features, and support boundaries. The practical lesson is to compare the actual commitments for the proposed service and workload. A government branding label is not sufficient evidence that every connected application or support channel is suitable. [3, 4]

Neither GCC nor GCC High is a certificate for the organization using it. A tenant may provide useful capabilities while its customer still uses weak access practices, unmanaged laptops, excessive sharing permissions, or inadequate incident procedures. Assessment examines the applicable organizational implementation and evidence. The product purchase is one part of that implementation, and the customer remains responsible for its own configuration and operation.

IJK should not assume that every Level 2 engagement automatically requires GCC High or that ordinary GCC necessarily satisfies every defense contract. The decision depends on the information, contract clauses, export restrictions where applicable, the specific cloud service boundary, and the commitments required from the provider. Some organizations may use another suitable architecture altogether. The team should record a reasoned choice, obtain necessary professional and contractual clarification, and verify the selected provider's current documentation.

Where DFARS 252.204-7012 applies to an external cloud storing, processing, or transmitting covered defense information, the contractor must ensure the provider meets the clause's FedRAMP Moderate-equivalent requirements and its specified incident-related obligations. A provider's general claim of security is not enough. The team needs evidence and contractual commitments for the actual service being used. [2]

This discussion is especially important when a customer says that it needs a compliant cloud. The parties should replace that broad phrase with an actual description of the workload and obligations. Email containing covered information, a separate file exchange portal, a backup repository, and a security log platform may all require distinct analysis. Approval of the primary collaboration tenant should not be treated as blanket approval for every service that exchanges data with it.

21.8 Deciding between the cloud environments

A migration that accounts for every dependency

EGH should maintain a migration workbook with a row for each workload and dependency, not merely a row for every mailbox. It records current location, proposed destination, data category, owner, volume, retention or hold, migration method, validation step, rollback option, and cutover window. Email, calendars, contacts, distribution groups, shared mailboxes, SharePoint permissions, OneDrive sharing, Teams channels, identity federation, application registrations, mobile devices, and desktop clients can each require different treatment. Audit history and legal holds must be considered before source data is removed. Harbor Point approves the business impact, and IJK verifies that it can support the resulting environment.

The pilot should include a typical engineer, an administrator, and a user who collaborates with an external partner. The engineer opens a protected drawing and checks that the application, permissions, and synchronization behavior match the design. The administrator confirms its approved role, MFA, logging, and recovery method. The external collaborator tests an allowed exchange without using a personal account or an unapproved transfer site. The pilot identifies failures in service availability, conditional access, mail routing, mobile enrollment, and customer collaboration while the population is still small. EGH records each failed test and its correction.

Cutover needs a rehearsal and a decision point. The team plans domain and mail changes, account activation, user communications, service-desk staffing, data freeze if required, validation, and a limited rollback window. A rollback is not simply moving a DNS record back when files have already changed in the new environment. The plan should say which data can be restored or reconciled, who can authorize a pause, and how users will avoid creating divergent records in two places. After cutover, IJK reconciles the expected people, devices, mailboxes, sites, log sources, backup jobs, and endpoint agents against what actually reports.

Third-party migration tools require the same scrutiny as the destination cloud. They may copy sensitive content, hold privileged credentials, create temporary repositories, or leave elevated application permissions. EGH should document the tool's hosting, access, data handling, license, retention, and removal plan. Microsoft documents limitations for certain native cross-tenant features in government clouds, including OneDrive migration; the chosen method must be tested for the specific source and

destination. The migration evidence should show both technical completeness and the disposition of temporary access and data. [7]

IJK should prepare a written decision record before purchasing subscriptions. The record should describe the information categories, relevant contract clauses, required collaboration partners, administrator locations, application dependencies, and expected support model. It should also identify which assumptions came from the customer, which came from contract review, and which require written confirmation from the cloud provider or reseller. This makes the decision explainable to future administrators and reviewers.

The team should compare complete operating arrangements, not merely monthly subscription prices. One option may require substantial migration work but reduce the complexity of meeting particular information handling conditions. Another may preserve existing integrations but require additional controls or a different protected workflow. An option that cannot support the organization's required customer interaction should be identified before it is purchased, rather than discovered when a project deadline is approaching.

GCC High should not be treated as a toggle that upgrades an existing commercial or GCC tenant in place. EGH should develop a migration plan that identifies what must be recreated, moved, reconfigured, or left behind. That plan should address identities, domains, email, shared workspaces, endpoint enrollment, applications, audit history, and external relationships. Actual migration methods and supported tools must be verified for the source and destination environments.

The benefits of either choice should be described in terms of the approved use case. Familiar collaboration capabilities can help employees perform their work, while an appropriate government service environment may provide commitments relevant to the organization's obligations. Those benefits are realized only when the selected features are available in the chosen cloud and are correctly licensed and configured. A feature demonstrated in a commercial tenant should be tested again in the government environment before acceptance.

The decision record should end with an owner and a review trigger. New export-controlled work, a major customer requirement, a new integration, or a material service change may require reexamination. IJK does not need to reconsider its entire architecture every time a user is added, but it must recognize changes that invalidate a previous assumption. EGH should transfer the reasoning behind the design so that IJK knows when to seek further review.

A defensible GCC or GCC High decision

The government cloud decision begins with a specific information flow. In a small engineering company, drawings may arrive through a prime contractor's portal, be reviewed in email, move into a SharePoint project site, synchronize to managed laptops, and be included in backups and incident records. If the team considers only the SharePoint destination, it can miss the mail gateway, desktop client, mobile device, backup platform, support ticket, or third-party application that receives the same information. EGH should map these paths with the customer, identify the regulatory or contractual basis for each restriction, and document what each proposed service will actually process.

GCC and GCC High are different Microsoft government service environments with different eligibility, architecture, service commitments, and feature availability. A customer should verify eligibility, service boundaries, support model, and the exact products it intends to buy. The choice does not turn every device, integration, and administrator into a compliant system. Nor does the phrase GCC High decide whether the information is export controlled or whether a particular application is suitable. Contract and data requirements must drive the selection, and the scope documentation must explain the resulting design. [3, 4]

An implementation plan must treat a move between cloud environments as a migration project. EGH should inventory mailboxes, domains, identities, groups, SharePoint sites, OneDrive files, Teams content, devices, applications, authentication methods, records holds, external sharing relationships, and audit evidence. It should test which migration methods actually support the source and target environments. Microsoft states that its native cross-tenant OneDrive migration feature does not support government cloud tenants, so an engineer must not promise that feature for a GCC or GCC High move without a currently supported alternative. [7]

The decision record should present the approved destination, rejected alternatives, conditions of use, owner, and review triggers in ordinary language. For example, leadership might approve GCC High for a particular controlled-workload boundary after confirming customer requirements, eligibility, migration feasibility, and the provider's commitments. That approval should name the workloads and connected services that were examined. A future backup provider, AI integration, customer portal, or cross-tenant collaboration change requires its own review; the earlier tenant decision does not automatically cover it.

21.9 Building a software and license register

The cost and evidence of each line item

A software register should begin with the question the product answers. The identity row describes the authoritative directory, authentication controls, administrator roles, recovery accounts, and assignment population. The endpoint row describes device management, detection, operating-system rights, and supported device classes. The audit row describes event sources, ingestion, retention, investigation, and expected cost drivers. The backup row describes protected data, restore objectives, encryption, location, and retrieval. The RMM and ticketing rows describe privileged reach and whether sensitive data enters their platforms. These capability descriptions prevent the register from becoming merely an alphabetized invoice list.

Each capability can involve several commercial relationships. Harbor Point may buy a government collaboration subscription through a reseller, IJK may bundle an endpoint product into a managed-service fee, and EGH may hold a time-limited migration-tool license. The register should state the legal purchaser, beneficiary, administrator, billing contact, support route, contract term, renewal notice date, and post-termination disposition for each. If a product is billed per user, the register names the covered users; if billed per device or server, it links to the corresponding inventory. A product that charges by log volume or backup storage needs a monitored utilization threshold and a person authorized to approve growth.

The source of entitlement evidence matters. A quotation describes an offer, an invoice shows a charge, a vendor portal shows a current entitlement, and an assignment export shows which identities or devices received it. Those documents answer different questions. EGH should reconcile them at acceptance, and IJK should reconcile them during operations. If a feature is configured but not licensed for a subset of users, the team corrects the purchase or changes the design before claiming full coverage. If a paid capability was never enabled, the team determines whether to configure it or remove unnecessary expense at renewal.

For Harbor Point's eight engineering users, a budget spreadsheet might begin with eight collaboration plans, but the actual purchase also considers managers, administrators, shared or service identities, endpoint and server coverage, backup workloads, logs, and support tools. A simple per-person price calculation can omit variable consumption and implementation labor. The first-year budget should show one-time migration and training separately from recurring license, monitoring,

support, evidence, and recovery costs. It should include a growth scenario and a provider transition scenario. Leadership can then understand whether the program remains affordable after EGH's project invoice has been paid.

Renewal should be treated as a security change. Thirty, sixty, or ninety days before a term ends, as appropriate to the vendor agreement, IJK verifies the actual utilization, continued need, exact replacement SKU, government-environment availability, and effect on controls. Harbor Point approves the spend and retains the decision. If the reseller proposes a different plan, the team maps every relied-on feature before agreeing. The register records the new terms and evidence of continuity. A missed renewal can disable an essential service as surely as a misconfigured firewall can.

CMMC specifies requirements to be satisfied, rather than a universal list of software brands to purchase. IJK should begin its software planning with capabilities such as identity management, access enforcement, device configuration, malicious code protection, audit review, vulnerability management, and incident response. It should then identify which existing tools already provide those capabilities and where additional products or services are necessary. This avoids paying twice for the same function while overlooking a responsibility that no product performs automatically.

A license register is the bridge between technical design and continuing operation. For each product, the register should record the exact vendor and product name, government cloud or hosting environment, purchased plan or SKU, licensed quantity, license metric, assignment method, subscription term, billing frequency, renewal date, and renewal owner. It should also identify the corresponding security capability, operating owner, support provider, and location of purchase and entitlement evidence.

The license metric matters because software is not always licensed per employee. Some products are licensed per user, others per device, server, workload, protected capacity, or volume of data processed. A security log platform may charge for ingestion and retention. A backup service may charge for protected users and additional storage. Server protection may require rights separate from workstation protection. The company should verify each metric in the actual quotation and licensing documentation rather than multiplying its head count by a single advertised price.

The register should also distinguish an available feature from a configured feature. A subscription may include an advanced capability that no administrator has enabled, while a deployed policy may depend on an entitlement that was never purchased for

all affected users. EGH should document both the right to use the feature and the settings through which it is implemented. IJK should review both after staff changes and renewal adjustments.

For the twenty-four-person example, the eight controlled-workload users provide a starting point for estimating collaboration subscriptions, but they do not settle the entire purchase. Administrators, shared resources, devices, servers, service accounts, and users benefiting from particular controls must be evaluated under the applicable licensing rules. A deliberate license review can uncover both overbuying and underlicensing. It should be completed before the final order and repeated when the architecture changes materially.

21.10 Collaboration subscriptions and the underlying platform

A purchase decision with verifiable entitlements

A reseller quotation should be translated into a capability schedule before it is signed. The schedule identifies each proposed plan or add-on, quantity, licensing unit, government environment, term, price basis, renewal rule, and the feature that the design relies upon. The feature column should describe a function such as conditional access, endpoint management, audit retention, or data loss prevention, not simply repeat the vendor's bundle name. EGH maps the configuration to an entitlement. IJK checks who will operate it and which identities or devices receive it. Harbor Point approves the recurring cost and keeps the evidence of purchase and assignment.

A useful review examines edge cases. An employee may use a managed workstation but hold only a basic collaboration plan; a privileged administrator may not be in the eight-person engineering group; a shared mailbox may have different rights from its delegates; a server may require separate endpoint protection; a mobile device may be managed only under particular enrollment conditions. The team should not infer licensing from job titles. It should identify the people and technical objects that use each capability and verify the current product terms. If a required security policy applies to ten people while only eight have the necessary entitlement, the gap is both a procurement and an implementation issue.

The subscription account needs an owner who can authorize additions and renewals. A reseller can transact the purchase and provide support, while Harbor Point should retain visibility into its tenant, domains, data, administrators, entitlements, and billing terms. If IJK pays for a platform and charges Harbor Point through a managed service, the service agreement should say whether the customer receives an individual

tenant or shared service, how fees change with head count or data volume, and what happens at termination. The invoice should permit Harbor Point to understand which essential controls it is funding without requiring disclosure of the MSP's unrelated commercial arrangements.

Entitlement review continues after purchase. Each month or other approved cadence, IJK compares the licensed population with active users and deployed features. It reviews expiring trials, disabled add-ons, unassigned subscriptions, unexpected growth, and product changes. It verifies that a renewal preserves the exact security capability used in the system security plan. A lower-cost plan can be a reasonable decision if the architecture is deliberately redesigned and retested; a silent downgrade that removes a control is not.

A collaboration subscription provides the services through which employees communicate and work with documents. In a Microsoft-centered design, this may include email, document storage, and collaboration applications. Microsoft 365 and Office 365 plan names should not be treated as interchangeable descriptions of identical rights. The exact government offering and associated security, management, desktop application, and operating system entitlements must be confirmed in the purchased plan.

EGH should turn the approved quotation into a service-by-service implementation plan. For email, that includes mailbox provisioning, authentication requirements, forwarding rules, approved recipients, and retention decisions. For document collaboration, it includes workspace ownership, membership approval, external sharing, versioning, and restrictions on uncontrolled synchronization. For meetings and chat, it includes whether sensitive material may be discussed, recorded, transcribed, downloaded, or shared externally under the approved design.

Installation is only one step. EGH should use a small pilot group to demonstrate that employees can complete their actual work within the controls. A project coordinator should be able to find an approved document, collaborate with an authorized colleague, and recover a previous version without moving the document to a personal account. A blocked action should have an understandable support process, so that users do not invent informal workarounds.

IJK maintains the platform by reviewing membership, external access, service health, configuration changes, and subscription assignments. It should also monitor service announcements that affect its government environment. Feature names and interfaces can change over time, and commercial-cloud instructions may not match the tenant

being operated. The maintenance guide should describe the policy objective and expected result as well as the current interface path.

The subscription continues according to its commercial terms. A monthly invoice does not necessarily mean the company has a month-to-month cancellation right. Annual commitments, renewal notice requirements, reseller conditions, and capacity additions need explicit review. IJK should preserve administrative access and billing visibility even when EGH places the order through an authorized reseller relationship.

Buying the complete capability rather than a familiar plan name

The first line of the purchase register should identify the collaboration foundation: the eligible government environment, the exact Microsoft 365 or Office 365 plan, number of licensed users, and the services required for mail, documents, meetings, and administration. A plan name is a starting point, not proof that every security function is included. EGH should map each designed feature to a current product term and government service description, identify any separate add-on, and verify that the feature is available in the chosen environment. IJK should retain the quotation, license terms, purchase record, assignment export, and a record of the configuration that uses the entitlement.

The second line of inquiry concerns identity. Each ordinary user needs an appropriate account and license for the services used. Privileged administrators may need additional identity capabilities, such as conditional access or time-limited privilege workflows, depending on the design and current entitlement rules. Emergency access accounts require their own control and monitoring design; they should not become an undocumented way around ordinary policy. The engineering team must test the real privileged paths, including service administration, endpoint management, remote support, and application consent, rather than testing only a standard employee sign-in.

Device management and endpoint protection form another purchase and coverage question. The proposal should distinguish management rights, operating-system rights, endpoint detection subscriptions, server protection, mobile-device coverage, and any workloads that rely on separate licensing. A license assigned to an employee does not necessarily cover a server, a shared kiosk, a contractor-owned laptop, or a disconnected engineering workstation. The purchased quantity should therefore be checked against a defined population of users, devices, and servers, with each exclusion explained.

Other capability lines may include email security, data loss prevention or information protection, audit retention, a security information and event management service, vulnerability scanning, backup, remote monitoring and management, ticketing, and a secrets vault. None is an automatic universal CMMC purchase. Each must answer a specific need in the approved architecture. The register should explain what data the product handles, where it runs, who administers it, what log or evidence it produces, which party pays for it, and how service continues if the reseller or installer leaves.

21.11 Identity protection and privileged access

An access request from approval to review

An engineer joins Harbor Point's controlled project on Monday. The program manager approves the business need and the data owner identifies the project resources the engineer may use. IJK receives a ticket that names the employee, manager, requested groups, start date, device, and any end date. The technician confirms the request's authenticity, creates or updates the individual identity, assigns the appropriate entitlement, and applies the approved authentication policy. An administrator should not infer the need for every project site from the engineer's job title. The completed ticket records the groups actually assigned, device status, person who performed the change, and any exception.

The first login is an acceptance test. The engineer reaches the intended workspace from a managed device using the approved authentication factors. The engineer cannot reach an unrelated project, and an unmanaged device fails the restricted path. IJK checks the identity and device logs to confirm what happened, then closes the onboarding ticket. If a manager requests an emergency exception because a deadline is near, the request moves to a named decision maker and receives an expiry and compensating process if permitted. The technician should not convert a one-day workaround into indefinite access by leaving a broad group assignment in place.

Privilege is a separate issue. EGH might temporarily need a tenant role to configure migration settings, while an IJK administrator needs a recurring but narrow role to manage devices. The roles should be assigned to named identities and activated under the approved method, with MFA, logging, and review. A service account used by an application needs an owner, a defined purpose, noninteractive restrictions where possible, credential or certificate management, and a retirement process. The emergency account should be protected and monitored through a specific procedure.

A control statement that says all administrators use MFA is incomplete if it ignores a legacy API key or unrestricted delegated relationship.

At the next access review, Harbor Point's manager confirms whether the engineer still belongs to the project. IJK provides a current export of group membership and privileged assignments and helps resolve discrepancies. A review record should show the population examined, reviewer, decisions, removals, and validation. A signature on a spreadsheet without checking the real directory has little value. If the engineer leaves, the offboarding trigger should reach IJK promptly, and the operator should revoke sessions, remove applications and group access, address the device, and review any shared secrets. The record links the manager's decision with the technical result.

A customer may ask IJK for proof of these actions during an assessment. IJK should be able to provide a sanitized but traceable sample of the request, approval, identity change, review, and closure through the agreed evidence channel. ABC can examine that chain within its authorized assessment. EGH's initial configuration explains how the rule was designed; ongoing tickets show whether Harbor Point and IJK actually follow it. The distinction matters because a perfectly configured identity platform can still contain access that no authorized person has reviewed.

Identity management controls who may enter the environment and what that person or application may do. Microsoft Entra ID is one possible identity platform in a Microsoft-centered design. The required plan depends on the features being used, such as conditional access, privileged access workflows, or particular identity governance capabilities. The team should verify availability and entitlements for the selected government environment rather than assuming every advanced identity feature is included in a base subscription.

EGH should create named administrative accounts separate from ordinary productivity accounts. Administrative roles should be assigned according to actual duties, and broad privileges should not become the default simply because they make installation easier. During implementation, temporary access may be necessary, but its purpose, approver, and expiration should be recorded. IJK must know which installer accounts exist and how those accounts will be removed or reduced at handover.

Multifactor authentication should be implemented through methods appropriate to the organization's requirements and supported environment. The deployment must address enrollment, lost authenticators, recovery, replacement, and the prevention of

unauthorized resets. A strong sign-in method can be undermined by a help desk process that accepts an unverified telephone request. IJK should train administrators to verify identity through approved procedures before modifying authentication methods.

Conditional access can enforce contextual rules, such as requiring an appropriately managed device for a protected application. EGH should test such policies in stages, using the platform's available evaluation features where appropriate, before broad enforcement. The test plan should include an authorized user, an unauthorized user, a managed device, an unmanaged device, and a recovery scenario. A policy that locks out both administrators on a Friday evening is an implementation failure even if the intended restriction was sensible.

Emergency access arrangements require special attention. IJK needs a tested method to regain control if its normal authentication dependency fails. Emergency accounts should be tightly controlled, monitored, and used only under documented circumstances, with exceptions limited and justified in the design. Credentials should not be stored in an ordinary shared document, and an account should not remain invisible to monitoring simply because it exists for emergencies.

After handover, IJK reviews privileged assignments, inactive identities, service principals, application permissions, and authentication exceptions. A scheduled review should record both the population examined and the decisions made. When access is removed, the evidence should show that removal occurred. The operating goal is to keep identity privileges aligned with current responsibilities, not merely to retain a screenshot of a secure configuration from installation day.

21.12 Endpoint management and operating system rights

A device that falls out of coverage

A recurring health review finds a laptop in Harbor Point's asset register but absent from the endpoint detection console. The technician first determines whether the inventory is current: perhaps the device was retired, perhaps the agent failed, or perhaps it was reimaged and never re-enrolled. The user reports that the laptop remains in use and has opened controlled drawings that week. IJK treats the missing protection as an active exception, not as a formatting discrepancy in a report. The team identifies the last known healthy check-in, installed version, connectivity, policy assignment, and whether any alerts or logs from that device are unavailable.

The correction must address the cause. If a rebuild script installed the management agent but omitted endpoint detection, IJK fixes the script and checks every device rebuilt with it. If a license limit blocked activation, the billing owner arranges sufficient entitlement and verifies that monitoring resumed. If a specialized application conflicts with the agent, the technical lead and Harbor Point assess supported alternatives and the impact on scope and business work. The operator records the interim treatment, owner, deadline, and validation. A screenshot showing the device present after one reboot is weaker than a subsequent health check and a repaired onboarding process.

The device inventory should reconcile several sources. Procurement records tell the team what was bought; the asset register says what is assigned; identity and management services show enrolled devices; endpoint security shows active sensors; vulnerability tools show scan coverage. None alone is authoritative for every question. IJK defines which source controls each field and documents legitimate differences, such as a spare computer powered off in storage. A weekly automated comparison can flag missing agents, but a human still needs to decide whether each discrepancy is a defect, a documented exclusion, or an obsolete record.

Operating-system and management rights should be checked during the same review. A device can continue to receive mail while losing the management entitlement used for compliance policy. A server may need a separate protection product. A contractor-owned device may be outside the standard enrollment model. EGH's original design should specify the treatment for those categories, and IJK should maintain it when devices change. Harbor Point approves any change that alters how the controlled work is performed. The management report names unresolved uncovered devices, not merely the percentage reported by the vendor dashboard.

When ABC samples one engineer's workstation, the evidence should connect the asset record, assigned user, approved baseline, encryption state, endpoint health, recent updates, and any exception history. IJK should be able to explain how it knows the larger population is covered. It need not claim that no device ever fails; it should show that failures are detected, evaluated, corrected, and used to improve the process. The sampling record should be current and tied to the assessed system rather than pulled from an unrelated customer tenant.

The lifecycle of an engineering laptop

Before Harbor Point buys a laptop, its asset owner determines whether the device will handle the controlled project, what applications it must run, and whether it can meet the approved operating-system and security baseline. IJK checks the intended management method, encryption, local administrator restrictions, endpoint protection support, backup coverage, and recovery process. EGH should test the selected management and protection features during implementation, but Harbor Point should own the purchasing decision and expected lifespan. A discounted device that cannot run the required engineering software and security agent is not a saving when it later requires an exception or replacement.

At receipt, IJK records serial number, owner, assigned user, intended scope, warranty, configuration version, and disposal route. It installs or enrolls the device through a controlled process, applies approved policies, confirms the operating-system license and required user or device entitlements, and tests the user's normal application. The device is not accepted because it appears in one management console. The acceptance record confirms identity enrollment, disk encryption, endpoint sensor health, patch baseline, logging, and any required backup or file synchronization. It identifies who validated the result and where the evidence is held.

During operation, changes to the laptop are linked to the asset record. If the engineer moves to another project, IJK reviews group membership and file permissions. If the device stops reporting, the service desk checks whether it is offline, retired, misconfigured, or missing a security agent. If it is lost, IJK initiates the incident and remote-action process according to the actual capability and circumstances. A dashboard showing ninety-nine protected devices out of one hundred is useful only if the missing device is named and its exposure is understood.

At retirement, IJK removes access and management assignments, preserves records subject to retention or investigation, confirms data transfer or destruction by an approved method, updates the inventory, and reclaims reusable entitlements. Harbor Point authorizes disposal where it owns the equipment. EGH should have no continuing device control unless a separate agreement gives it a defined support role. The lifecycle record ties the original purchase, installed controls, operating exceptions, and final disposition together.

Endpoint management applies approved settings to computers and, where included in the design, mobile devices. Microsoft Intune is one possible management platform. Its government service documentation identifies environment-specific details that

must be considered when designing enrollment and administration. EGH should verify the supported endpoints, features, and licensing for the chosen cloud before promising identical behavior to a commercial deployment. [5]

A device should enter service through a defined enrollment process. The process identifies the owner, records the asset, verifies the operating system and support status, applies the approved configuration, and confirms that required security tools report correctly. Merely displaying the device in a management console does not establish that all policies have arrived or succeeded. EGH should verify configuration results and resolve conflicts before giving the device to a controlled-workload user.

The operating system itself requires appropriate licensing and technical capability. A Microsoft subscription may provide particular upgrade or management rights subject to qualifying conditions; it should not be assumed to replace every underlying Windows license. The purchaser must confirm the qualifying base license, edition, and permitted use. Servers, virtual machines, remote desktop access, and virtual desktop services may have additional rights and costs that do not follow automatically from workstation licensing.

Device encryption should be configured with an approved recovery process. IJK needs to know where recovery information is stored, who may retrieve it, how retrieval is logged, and how a lost device is handled. Where FIPS-validated cryptography is required, the organization should verify the cryptographic module, supported version, and operating configuration. A marketing statement that a product uses strong encryption does not by itself demonstrate the required validation or mode of operation.

IJK maintains endpoints by reviewing enrollment failures, unsupported versions, missing updates, encryption state, local administrator privileges, and configuration drift. Devices that have not checked in require investigation rather than automatic dismissal as inactive. The employee may be on leave, the computer may be broken, or the management agent may have been disabled. Each explanation requires an appropriate recorded action.

When an employee leaves or a device is retired, the process must address both access and stored information. Revoking a cloud session does not necessarily erase locally stored material. IJK should recover or appropriately wipe the device, preserve required records, remove obsolete assignments, and update the inventory. Disposal and sanitization decisions should follow the organization's approved media procedures and applicable obligations.

21.13 Endpoint detection and response

A vendor outage and a backup detection method

During a vendor service outage, endpoint agents continue running locally but stop reporting to IJK's central console. The team first establishes which devices are affected and when visibility was lost. It contacts the vendor, preserves the notice and status updates, and checks whether local protection and isolation functions still operate. IJK informs Harbor Point according to the service agreement if the loss of visibility materially affects the protected environment. A vendor's public incident page is useful context but does not establish the state of Harbor Point's particular devices. IJK compares the expected asset population with last check-in times and records the difference.

The operating procedure should define alternative observations. Identity sign-ins, network events, local device logs, RMM health, and user reports may offer partial visibility during the outage. None should be described as a complete substitute without testing. IJK can restrict a high-risk change, increase manual review, or take another approved measure while central telemetry is unavailable. Harbor Point decides whether a business process should pause. EGH may advise on a recently installed integration under its support terms, but it does not become the incident owner by default.

When the vendor service returns, the team verifies that the agent population reconnects, delayed alerts are delivered or recovered, policies remain assigned, and any configuration changes made during the outage are understood. A test event checks the alert-to-ticket path. IJK reviews the blind interval for suspicious activity using available records and documents limitations. The management report states the duration, affected population, interim measures, and validation. A final green dashboard is not proof that the missing hours were covered.

The contract and license register should support this response. It identifies the vendor support route, status channel, service commitment, export capability, and escalation contact. The monitoring design should identify which failures generate an alert independent of the affected service when feasible. Harbor Point can then evaluate whether its architecture provides enough resilience for the controlled work and whether a different service or supplemental process is justified.

What an endpoint alert must produce

Suppose an endpoint sensor detects a suspicious script on an engineer's laptop. The alert should identify the device, account, time, process, and relevant context in a console that IJK can access. The first analyst validates that the device belongs to Harbor Point's protected population and assesses whether the event is a known administrative action or possible compromise. The analyst opens an investigation record rather than closing it solely because the tool assigned a low severity. An approved EGH migration script can still be misused, and a low-confidence signal can matter when paired with a privileged sign-in or unusual file transfer.

IJK's response procedure specifies when it may isolate the endpoint, who receives notice, and what evidence to collect before actions change the system. Harbor Point may have business reasons to keep an engineering application available, but those reasons need to be weighed against exposure and contractual obligations. The operator records the evidence available at each decision, then documents containment, analysis, eradication, recovery, and follow-up. If the event is reportable under an applicable clause, Harbor Point's authorized lead coordinates submission while IJK supplies facts and preservation support.

Coverage reports need independent population checks. EGH's acceptance test demonstrates the agent on pilot devices, but IJK maintains the comparison between the asset inventory and active sensors after handover. It reviews devices that have not checked in, agents that cannot update, and policies accidentally assigned to a weak group. A subscription may expire while the console remains accessible, so the license register and health check must cover entitlement as well as telemetry. Servers and specialized devices receive documented treatment based on actual support and design rather than being omitted from a user-only report.

The evidence of a successful endpoint program is not a promise of zero alerts. It is a traceable pattern of coverage, timely triage, justified decisions, corrective work, and management awareness of significant gaps. A sampled case should let a reviewer see the original signal, the analyst's reasoning, the actions taken, and the eventual validation. Harbor Point should be able to explain who owns those records when IJK's analyst changes jobs or the endpoint vendor is replaced.

Endpoint protection helps detect and respond to suspicious behavior on computers and servers. Endpoint Detection and Response, or EDR, adds investigative and response capabilities beyond a simple statement that antivirus is installed. Microsoft Defender for Endpoint is one possible product, with separate government

environment guidance. Alternative products may be appropriate if their capabilities, hosting, information handling, and support arrangements meet the organization's needs. [6]

Before deployment, EGH should determine whether the license covers workstations, servers, or both, and whether the desired response features are included. The team should understand what data the agent collects and where it sends that data. Process information, file paths, user identifiers, and collected files can create additional information handling considerations. A tool should not be approved solely because its purpose is security.

Installation should include onboarding, policy configuration, protection against unauthorized tampering where supported, and alert routing. EGH should demonstrate a vendor-supported benign test that proves an expected detection reaches the intended operator. The test should also establish whether the operator can investigate and perform an authorized containment action. A successful installation without a tested response path leaves a gap between detection and action.

IJK must decide who reviews alerts and when. If the company cannot provide continuous coverage, it should establish a realistic after-hours arrangement and evaluate whether a managed detection and response service is necessary. A twenty-four-hour service should be defined by actual staffing, escalation commitments, and response authority. Buying EDR software alone does not purchase a continuously staffed security operations center.

The response authority should be specific. An operator may be permitted to isolate a suspected compromised laptop immediately, while stopping a production server may require additional escalation. The procedure should identify who can authorize action when the primary leader is unavailable. Decisions and actions should be recorded so the company can reconstruct what happened and improve its response process.

Maintenance includes checking agent health, coverage against the asset inventory, exclusions, unresolved alerts, and changes to detection policy. Broad exclusions introduced to make an application work should receive particular scrutiny. EGH should transfer the reason for every approved exclusion, and IJK should periodically confirm that it remains necessary. Otherwise, temporary troubleshooting decisions can become permanent blind spots.

A line-by-line example of the license decision

Consider a proposed order that includes eight government collaboration subscriptions for the engineering group and two subscriptions for managers. The first check is whether those users need distinct plans because of their actual features and access, and whether other employees can reach controlled information through shared mailboxes or files. The second check is whether the chosen plan carries the identity, device-management, endpoint-protection, audit, and information-protection entitlements used in the design. Where an add-on is required, its assignment population must be explicit. The register should not claim that ten collaboration licenses automatically protect every server, administrator, scanner, and backup workload.

A proposal might name Microsoft 365 Government G3 or G5, Office 365 Government G3 or G5, and separate security offerings. Those plan families have different bundled rights, and availability can differ between GCC and GCC High. The installer should produce an entitlement matrix from the current government product terms and service descriptions for the actual quote. The matrix names the capability, plan or add-on that grants it, licensing unit, covered population, configuration to be deployed, and evidence of assignment. EGH and the reseller validate purchase rights; IJK validates that every operated device and user is covered; Harbor Point approves cost and contract term. [3, 4]

A separate budget line may be necessary for servers, SIEM ingestion, long-term log retention, backup storage, vulnerability scanning, an RMM platform, a ticketing system, and a secrets vault. The list is an architectural analysis, not a mandatory vendor basket. For each proposed external service, Harbor Point and IJK ask whether it receives CUI, security protection data, credentials, or only ordinary business records, and whether the provider's commitments support the intended use. An inexpensive product can be expensive in practice if its data location, support access, or evidence export cannot be reconciled with the protected workflow.

The first-year cost model should separate one-time discovery and migration work from recurring subscriptions and operating labor. It should account for onboarding, acceptance testing, administrator training, help desk procedures, routine reviews, restore exercises, incident support, evidence management, renewals, and provider transition. It should show the effect of adding five employees, doubling log volume, replacing a server, or extending retention. Harbor Point can then decide whether its

planned work supports the continuing expense rather than approving an implementation price that omits operation after EGH leaves.

21.14 Email protection and information protection

A mistaken external share

An engineer intends to send an approved project summary to a prime contact but selects a similarly named outside address. An information-protection policy may warn, block, or log the action depending on the design. IJK investigates the event and preserves the relevant message metadata and policy result. Harbor Point's data owner determines whether regulated information was included and who must be notified. EGH's implementation record shows which policy was configured, while actual event logs show what happened. The response should not assume the tool prevented disclosure merely because the policy exists.

The preventive process begins before the message. Harbor Point's approved collaboration workflow defines which recipients and channels are permitted, how external identities are verified, and how employees label and review content. EGH configures the selected controls in the actual government environment and tests representative cases. IJK maintains policy assignments, handles false positives, and checks that new users and groups receive the intended settings. If the tool lacks a required capability in the chosen plan or cloud, the organization needs a tested alternate method and corresponding training.

The incident analysis examines whether the message left the approved boundary, whether the recipient opened it, what information it contained, and whether copies remain. Harbor Point applies its contract, incident, and customer notification processes based on verified facts. IJK assists with technical containment such as revoking a link when supported, while preserving evidence. A deletion request to a recipient may be appropriate but should not be treated as proof that no disclosure occurred. The record distinguishes prevention, detection, and response.

The lessons may change both technology and behavior. Perhaps the directory displays confusing contacts, the sharing process lacks recipient verification, or the data owner never defined what may be sent externally. Harbor Point approves the new workflow, IJK adjusts controls and training, and EGH helps only if engaged for a technical change. The monthly report captures corrective decisions without reproducing sensitive content for a broad audience.

Email security addresses risks such as phishing, malicious attachments, impersonation, and unauthorized forwarding. A base email subscription and an advanced email protection plan may provide different capabilities. IJK should identify the protections required by its design and confirm the entitlement for each feature. It should also verify whether the proposed feature exists in the selected government environment and whether it applies to all intended users and mail flows.

EGH should configure authentication and mail flow controls in a coordinated way. Domain-related settings such as SPF, DKIM, and DMARC require an accurate understanding of legitimate sending systems. A payroll service, customer portal, or line-of-business application may send mail for the organization. The team should inventory these senders, test expected behavior, and move toward enforcement without silently breaking necessary business messages.

Information protection tools, including selected Microsoft Purview capabilities where available and appropriately licensed, can help classify information and enforce handling rules. A sensitivity label should have a defined business meaning and a tested technical effect. Employees need to understand whether the label changes access, applies encryption, restricts sharing, or simply marks the document. Applying a label does not independently determine whether the document is CUI.

Data Loss Prevention, or DLP, can detect certain patterns and restrict particular transfers, but it depends on the policy design and supported locations. A rule may behave differently in email, document storage, and endpoints. EGH should test representative permitted and prohibited workflows using non-sensitive test material. The test record should show what was attempted, what happened, and whether an alert reached the person responsible for follow-up.

IJK maintains these controls by reviewing exceptions, false positives, unprotected locations, and user behavior. If legitimate work is repeatedly blocked, the company should improve the approved workflow rather than quietly disabling the rule. If sensitive information is leaving through an unmonitored application, the architecture requires correction. Training, access design, and technical enforcement need to support the same handling decisions.

21.15 Audit logs and security monitoring

A missing log source during a normal week

On Wednesday, IJK's monitoring dashboard reports that Harbor Point's backup platform has stopped sending administrative events. No attack alert has fired, and scheduled backups still show success. The analyst checks the log-source inventory and sees that changes to backup policies and privileged access are expected in the security monitoring service. The absence of events is therefore itself a control-health problem. The analyst opens a case, confirms the last event received, checks whether the backup vendor changed an API permission, and alerts the technical owner. The team should not wait until an assessment request discovers the gap.

The response depends on cause and exposure. If a token expired, IJK replaces it under change control and verifies the connector with a test event. If the vendor changed an event format, IJK adjusts parsing and checks whether the missing period can be retrieved from the source. If the source retained no events, the team records the interval and considers what it could not observe. Harbor Point's manager receives a material exception report if the gap affects a relied-on control. EGH helps only if the connector remains within a covered implementation defect or a separate support agreement.

The analyst's record should state the expected source, failed period, cause, corrective action, recovered data if any, validation, and whether related sources were checked. It should avoid creating a false impression that the monitoring was continuous during the gap. A screenshot of the restored connector shows current function but does not prove events existed during the outage. The system security plan may need an update if the original design assumed a different retention or alert mechanism. Management can then make a sound decision about additional collection or process changes.

Capacity introduces another failure mode. A log service may receive every event but stop retaining older material because the purchased capacity is insufficient. IJK's register should define expected ingestion, retention, alerting when thresholds are near, budget owner, and action before a limit is reached. It should consider source criticality and contractual obligations rather than blindly lowering collection. If Harbor Point adds servers or a new remote access platform, the change request includes log growth and integration tests. The security team should understand the financial consequence before the monthly invoice surprises management.

ABC may later test monitoring by asking an operator to locate a specified event and explain the subsequent response. IJK should demonstrate the source record, ingestion, alert or query, investigation ticket, and disposition. A policy that promises continuous monitoring cannot be supported by a console license alone. The ordinary missing-source case demonstrates that the organization monitors the monitoring system itself, which is often the difference between a design on paper and a dependable operation.

From log collection to an investigated event

A log architecture starts with the questions the organization needs to answer. Can it identify a privileged role grant, a failed administrator sign-in, a device that stops reporting, a file shared outside the approved group, or a backup configuration change? For each question, EGH identifies the authoritative event source, collection path, retention arrangement, alert logic, and evidence export. IJK determines who sees the alert, how quickly it must be triaged under the service agreement, how an investigation is recorded, and when Harbor Point must be told. The design should account for events generated by the cloud tenant, endpoints, network devices, RMM, backup, and relevant third-party services.

A connector marked healthy is only one part of validation. EGH can generate a controlled test event, verify its timestamp and identity in the source, confirm ingestion into the monitoring platform, trigger the expected alert, and inspect the ticket and escalation. IJK should repeat representative tests after configuration changes and compare the source inventory with ingestion health. A log source can disappear silently when a license changes, a certificate expires, a device is replaced, or an API permission is withdrawn. A monthly source-health report should show both the expected and observed population.

Retention and cost are connected. Some platforms charge by ingest volume, storage, or query capacity. Harbor Point and IJK should identify which records need to be retained under the applicable contract, assessment evidence plan, incident process, and organizational policy. They should avoid turning a specific ninety-day incident preservation requirement into a general ninety-day log-setting assumption. They should estimate normal volume and growth, monitor actual use, and specify what happens when a limit is reached. Dropping required events to avoid a bill without approving a compliant alternative is a serious design change. [2]

The investigation record should preserve the original alert, scope of review, relevant queries or exports, actions taken, people notified, and conclusion. A false positive

still deserves enough context to show why it was closed. A true event needs escalation and preservation under the incident plan. ABC may later sample such records to examine whether monitoring is operating. It should see ordinary records generated before the assessment was scheduled, not a folder of newly staged examples.

Audit records help an organization determine who performed an action, when it occurred, and what system or information was affected. Useful records may come from identity services, endpoints, collaboration platforms, firewalls, administrative tools, and backup systems. A Security Information and Event Management platform, or SIEM, can consolidate and analyze these records. Microsoft Sentinel is one possible implementation, but its environment support, data handling, and charging model must be verified for the design.

The first logging decision is what the organization needs to observe. IJK should identify events relevant to unauthorized access, privilege changes, security configuration changes, suspicious file activity, and failures of protective services. Collecting everything without a review plan can create substantial cost and still fail to produce a useful response. Conversely, collecting only inexpensive records may omit the events needed to investigate a compromise.

EGH should document each source, connector, destination, time synchronization dependency, retention setting, and expected delivery delay. It should test whether records arrive with the fields needed for investigation. A dashboard showing a green connector status is not enough if important event categories were never enabled. The acceptance test should generate representative activity and trace it from the originating service to the review location.

Retention requires several separate decisions. Searchable retention, archived retention, incident preservation, and assessment evidence retention serve different purposes. IJK should establish periods based on applicable requirements, investigation needs, and documented policy. It should not assume that a platform's default audit retention satisfies every obligation, or that a ninety-day incident preservation rule means all ordinary security logs should be deleted after ninety days.

Costs should be modeled using expected data volume and growth. An unusually verbose source can increase ingestion charges quickly, while an expired add-on can reduce access to historical records. IJK should review usage and cost together with coverage. The objective is a sustainable monitoring design that preserves necessary

evidence and produces actionable information, rather than an impressive collection of logs that no one reviews.

21.16 Vulnerability management and patching

A legacy application with no quick patch

Harbor Point relies on a specialized engineering application that only works on an older supported configuration. An authenticated scan finds a vulnerable component, but a direct vendor update breaks the application in a test environment. IJK documents the affected devices, software version, exposure paths, available fixes, and business use. Harbor Point asks the application vendor for a supported path and determines whether replacement, isolation, restricted access, or a different workflow is feasible. EGH may design a technical change if its agreement covers the work. No party should close the finding simply because the patch cannot be installed today.

An interim plan should be specific and testable. It might limit the device's network paths, remove unnecessary administrative rights, increase monitoring, restrict which users can operate it, and prevent controlled information from entering an unsupported feature. IJK verifies the restrictions and records their operation. Harbor Point approves the business disruption and funds a replacement or migration plan. The system security plan and exception register describe the real implementation, including what remains unfulfilled. Management's acceptance of a business risk does not alter an external requirement or a program's rules for allowable remediation.

The long-term plan identifies milestones: vendor support decision, application testing, equipment purchase, pilot, data migration, user training, and retirement of the old device. Each milestone has an owner, date, and evidence. If Harbor Point obtains a new contract that increases use of the application, the plan is reevaluated before adding more affected devices. A scheduled scan and manual inventory review check for the same component elsewhere. IJK validates final remediation with a rescan or equivalent technical test.

ABC may examine the condition during an assessment. The organization should present accurate documentation and evidence rather than a screenshot of a temporary rule without context. The assessment outcome depends on the applicable requirement and rules; the textbook cannot promise that an interim control will be accepted. The teaching point is that a difficult dependency needs engineering, management, and candid evidence, not a hidden scanner exclusion.

One finding from discovery through verification

Suppose an authenticated scan identifies a vulnerable engineering workstation. The first step is to verify that the finding applies to the actual device and installed software. IJK checks the asset owner, exposure, available fix, and whether exploitation is known. EGH may help if the issue stems from the recently installed baseline, while Harbor Point's business owner explains whether the device is needed for a deadline. A finding should not be closed merely because the scanner stopped seeing a powered-off machine. The team records the affected population and searches for the same weakness elsewhere.

The change owner prepares the update. If the vendor offers a patch, IJK tests it against a representative application and schedules deployment under the approved process. If the patch disrupts an engineering tool, the team documents the failure, available alternatives, interim restrictions, and a new validation date. Harbor Point approves the business impact of downtime or replacement. An internal exception is a management decision and does not automatically satisfy an external security requirement. The system security plan and remediation records should reflect what is actually operating, not the configuration that was originally intended.

After deployment, IJK verifies installation on every affected device, rescans where appropriate, and checks that the normal application and protection agents still function. It attaches the verification to the change and finding records. The reporting packet shows open findings, age, ownership, and trends by population. A dashboard percentage can be useful if its denominator is known. It is misleading if disconnected devices, servers, or subcontractor endpoints have been quietly excluded without a scope rationale.

Patch management is one piece of configuration management. A new operating-system build can alter identity integration, endpoint protection, encryption, backup, or logging. EGH's installation baseline therefore needs an owner after acceptance, and IJK needs a controlled way to update it. Quarterly or other internally selected reviews can compare the approved baseline with a sample of real systems. A failed comparison triggers investigation, correction, and documentation instead of rewriting the baseline to make every deviation disappear.

Vulnerability management identifies weaknesses, evaluates their significance, and follows remediation through verification. A scanner is one component of that process. The organization also needs a reliable asset inventory, authorized scanning methods, a treatment workflow, exception handling, and a way to confirm that fixes worked.

Open-source or commercially licensed tools may be suitable, but their operation and information handling must fit the environment.

EGH should establish the initial scanning coverage and explain how authenticated scans are performed where appropriate. Credentials used for scanning require protection and controlled privileges. The team should confirm that scanning does not disrupt fragile systems and that excluded assets are visible in the risk and scope records. A clean report from an incomplete scan should not be presented as evidence that the entire environment is free of vulnerabilities.

IJK should prioritize findings by considering exposure, exploitability, business function, information sensitivity, and available treatment. A numerical severity score is useful, but it does not replace judgment about an exposed service or a vulnerability actively being exploited. The organization's remediation deadlines should be documented and achievable, with escalation when a deadline cannot be met. Such internal deadlines should be clearly distinguished from any externally mandated requirement.

Patch management should include testing, deployment, failure review, and confirmation. A tool reporting that an update was offered is not necessarily evidence that the device installed it and restarted successfully. IJK should identify devices that remain behind, determine why, and document the corrective action. Unsupported operating systems and applications require a replacement or other appropriate treatment plan because ordinary patching may no longer be available.

Exceptions should have an owner, reason, compensating measures where applicable, and a review date. For example, a business application may temporarily require an older component, but the exception should describe how exposure is reduced and when the dependency will be removed. An internal exception does not make an unmet assessment requirement acceptable. Before assessment, the team must evaluate the actual requirement and any permitted formal treatment under the applicable rules.

21.17 Backup and recovery services

Recovery when the usual administrator is unavailable

A credible recovery exercise assumes the administrator who built the backup job is absent. Harbor Point declares that a project repository needs restoration to a clean location. An alternate IJK operator consults the runbook, obtains authorized approval, locates the backup, retrieves the required key through the approved vault process, and

restores a representative data set. The operator verifies content, timestamps, project permissions, and the ability of the engineering application to open the files. If the procedure requires calling EGH after its stabilization period, the exercise has identified an unresolved dependency, even if the data itself was preserved.

The test should record the recovery point selected, elapsed time, observed data loss, applications restored, permissions, errors, and business validation. Harbor Point compares the result with its recovery objectives. A successful small-file restore does not prove that a complete server, repository, or identity service can be recovered within the same period, so the plan should use several representative test types over time. IJK can schedule these tests under its service agreement and escalate failures. EGH's original acceptance test provides a baseline, while later tests show ongoing capability.

A compromised administrator changes the recovery sequence. The team may need to prevent the attacker from reaching backup credentials, preserve incident evidence, identify a clean recovery point, rotate secrets, and rebuild management access before restoring data. A backup console accessible with the same compromised identity as the production tenant may be a single point of failure. EGH's design should explain separation and key custody; IJK should periodically test those assumptions. Harbor Point decides which business services recover first and who may declare that regulated work can resume.

Provider termination is also a recovery problem. If backup storage or software belongs to IJK, Harbor Point needs a contractual route to its information when it changes MSPs. The parties should know the export method, fees, retention window, encryption-key ownership, and deletion evidence. If the vendor itself fails, an alternate copy or recovery path may be needed according to the approved design. The point is not to buy every possible redundancy. It is to understand what failure the current architecture can survive and what evidence supports that understanding.

The monthly report should therefore distinguish job completion, coverage, restore testing, and unresolved recoverability risks. A backup job can finish every night while a critical data set is excluded or inaccessible after restoration. Management needs a clear explanation of which workloads were tested, the result, and the next planned test. ABC may examine selected records during assessment, but it does not take over the recovery process. IJK remains the operator and Harbor Point remains the owner of business recovery decisions.

Proving restoration across both data and authority

Backup selection begins with the data and recovery objectives. Harbor Point identifies the critical project files, mail, configuration records, and other workloads; it states how much loss and downtime it can tolerate and who may authorize restoration. EGH designs coverage, destination, encryption, access, retention, and separation from the primary environment. IJK operates the jobs and tests recovery. The vendor may supply storage and software, but its service description should not be mistaken for Harbor Point's own recovery plan. A successful overnight job is evidence that copying occurred, not that the business can resume.

A representative restore test should name the source, point in time, destination, operator, expected permissions, and validation criteria. For example, IJK restores a project folder into an isolated location, confirms file integrity and access only by the approved engineer group, and records the result. Another test might recover a configuration or an entire workload. If encryption keys, identity service, or the backup console are unavailable during the incident, the team needs a route that does not depend entirely on the failed system. EGH should demonstrate that route at handover and transfer the necessary knowledge securely.

Backup data can itself contain CUI or other sensitive information. The team documents the provider, storage environment, administration, support access, transfer path, and deletion at contract end. A secondary copy in an ordinary commercial repository may undo careful design of the primary GCC High workspace. Harbor Point and IJK should evaluate the applicable cloud and contract obligations for the actual backup service rather than assuming the primary tenant's commitments extend to a different provider. Restore testing should not expose real sensitive data to an uncontrolled test machine.

After a ransomware event, recovery is a sequence of decisions. The incident lead determines what evidence to preserve, which systems are trustworthy, how credentials and keys will be secured, and whether restored files might reintroduce malicious content. Harbor Point authorizes business priorities; IJK executes the approved recovery; EGH assists only under an active agreement or separate authorization. The record should distinguish a successful restore from confirmation that the environment is safe to reconnect and resume regulated work.

Backup protects recoverability, while security controls protect the environment in other ways. Synchronization, replication, document versioning, and recycle bins can be helpful, but they should not be assumed to provide every recovery capability the

business needs. IJK should decide what must be recoverable, how far back recovery must reach, how quickly service must resume, and how recovery will work if the primary administrator's account is compromised.

Recovery Point Objective, or RPO, expresses the amount of data loss the business can tolerate, usually in time. Recovery Time Objective, or RTO, expresses the target time to restore an acceptable service. These are business decisions supported by technical design. A company that says it can tolerate only one hour of lost work should not purchase a solution that captures the relevant data only once each night without recognizing the mismatch.

Backup licensing may depend on users, workloads, protected capacity, storage consumption, or a combination of these. EGH should provide a bill of materials that covers the actual protected systems and retention design. If backup data contains CUI or covered defense information, the destination and provider arrangement must be evaluated accordingly. Moving a copy into a backup service creates another location requiring protection; it does not make the information less sensitive.

EGH should demonstrate a restore, not just a completed backup job. The test should use appropriate test material and show that authorized personnel can recover the content to an approved location with usable permissions. IJK should also understand how to recover when the production identity system is unavailable. Backup administrator access and recovery credentials should not depend entirely on the system the backup is intended to restore.

During operations, IJK reviews failed jobs, missing workloads, retention changes, storage growth, and restore results. Where immutable or otherwise protected copies are used, the team should verify the configured protection and the administrative paths that could undermine it. The company should periodically test a recovery scenario that reflects a meaningful business failure, such as a compromised administrator or an unavailable collaboration service.

Remote support as a controlled pathway

An MSP's remote support platform can reach far beyond the application that holds a drawing. A technician may be able to run a shell, transfer a file, see the user's screen, install software, or change a security setting. For Harbor Point, IJK should identify each access route, the operator identities permitted to use it, authentication controls, scope of the delegated role, session logging, approval for elevated actions, and emergency procedure. The review should include vendor support and subcontractors.

A statement that technicians do not ordinarily open CUI does not explain what they can do through a privileged tool.

The support workflow begins when a user opens an approved ticket. The ticket records the affected device, purpose, urgency, and any sensitive information the user might share. IJK authenticates with an individual account, applies the access level required for the task, and records significant changes. If a support session exposes a controlled drawing, the technician follows the agreed handling process rather than uploading an unrestricted screenshot to a commercial ticket portal. EGH should test that its installer support path follows these same boundaries during migration.

Temporary provider access needs an expiry mechanism. EGH may require high privilege to configure identity policies or migration tooling, but Harbor Point and IJK should know which accounts, enterprise applications, delegated admin relationships, API grants, certificates, and agents were created. The handover inventory should include them all. At acceptance, IJK verifies that a required stabilization path remains narrowly available for a defined term and that every other path has been disabled or revoked. A later maintenance request can grant new time-limited access through ordinary approval.

If the remote platform itself fails or is compromised, IJK needs a fallback that does not depend on the same credentials and infrastructure. The incident plan should state how technicians lose access, how customers are informed where required, and how systems can be reached for containment and recovery. Such an event can affect several customers simultaneously. The MSP's internal incident record and each customer's contractual reporting analysis remain separate, even while the technical response is coordinated.

21.18 Remote administration and supporting tools

Separating routine support from emergency power

The normal support path begins with an approved ticket and a named IJK technician. The technician uses an individual identity and a role limited to the customer's environment, confirms the device and user's identity, and records material actions. A remote session may expose controlled information on screen even if no file is downloaded. IJK should therefore train technicians on what they may capture, paste into tickets, or discuss on an unapproved channel. The ticketing platform's own data handling and provider commitments belong in the scope and service review where it can receive sensitive material.

Some tasks require elevated privileges. Rather than giving every support worker permanent broad access, IJK can establish an approval and time-bound activation process appropriate to its architecture. The record names the reason, target system, authorizer, activation and expiry, and change performed. The monitoring process should detect unexpected elevation and use by a departed technician. EGH may require similar access during implementation, but its accounts and permissions are identified separately so they can be closed at handover. A shared emergency account, if one is necessary, needs custody, logging, and review outside ordinary technician accounts.

The RMM platform deserves special treatment because it can execute commands across many devices. IJK should restrict scripts by role and customer, test them on a limited group, use approval for high-impact changes, and retain execution records. A script intended for Harbor Point should not be deployable to an unrelated customer group through a naming mistake. Vendor updates, technician turnover, and delegated third-party access can change the platform's risk. IJK reviews administration and integration regularly and maintains a way to disable or isolate the tool during a compromise.

Emergency access is practiced before an emergency. If the normal identity service is unavailable, the recovery account and support route should permit the approved team to restore service without creating an uncontrolled standing bypass. The exercise confirms who holds the credentials, how a second person is notified, which actions are logged locally or reconstructed afterward, and how access is reset. Harbor Point knows who can authorize extraordinary actions affecting its environment. A written procedure that no one has used is a weak substitute for a controlled test.

At provider transition, remote agents and delegated relationships are among the most easily forgotten pathways. Harbor Point and the replacement operator inventory every device agent, application consent, API token, support identity, vault permission, and certificate. They remove IJK's access after the new service has been validated and document disposition of IJK's copies of customer information. The same process applies to EGH at the end of installation. The absence of a named login does not prove a former provider has no technical route into the environment.

Remote Monitoring and Management software, commonly called RMM, can provide powerful access across many computers. That power makes its design particularly important for an MSP. A compromised RMM platform or broadly privileged technician account can create a path into multiple customer environments. IJK should

evaluate administrative separation, multifactor authentication, session controls, audit records, update security, and the provider's information handling before approving the tool.

EGH should configure remote support around named identities and approved authorization. Unattended access should be limited to justified systems and roles. The design should address whether file transfer, clipboard synchronization, remote printing, and session recording are permitted. These functions can move protected information outside its intended boundary, even when the remote tool is used for legitimate support.

Ticketing and documentation platforms also require review. A technician may paste an error message containing sensitive information into a ticket, upload a screenshot, or attach a configuration export. IJK should define what may be recorded in the ordinary service desk and where restricted material must be placed. A ticket can reference a protected evidence location without reproducing its contents in a less suitable system.

Password management should use an approved vault with role-based access, auditability, recovery planning, and appropriate hosting and contractual terms. Shared emergency secrets may be necessary in limited circumstances, but ordinary administrators should still use individual identities. The vault should not become a reason to preserve broad shared accounts that make individual accountability impossible.

Training platforms, secure file exchange tools, mobile management, network appliances, and policy management systems may add further licenses. Some organizations need dedicated products; others can satisfy their needs through capabilities already present in the approved environment. IJK should purchase a separate tool only when it resolves an identified requirement or operating need and when the company can maintain it. Every additional product brings its own access, update, evidence, and renewal obligations.

A complete entitlement and vendor register

A practical register should have one record per product and a separate record for major service components that share a subscription. For a government collaboration tenant, record the tenant identifier, legal account holder, eligible purchasing entity, billing owner, reseller, primary and backup administrators, contract term, renewal notice period, data export method, and locations of authoritative records. For an

endpoint product, record its vendor portal, protected population, deployment group, policy owner, alert recipient, license metric, and independent coverage check. For a backup platform, also record the protected workload, backup destination, restore-test owner, encryption key custody, and post-termination data treatment.

The register must distinguish title, entitlement, administration, and custody. IJK may own the tenant and subscribe to the services while EGH temporarily administers them. The software vendor owns its product and grants rights under the license; EGH's status as reseller does not make it the owner of IJK's data. A customer may own its own tenant while IJK receives delegated administrative access under a service agreement. These are different relationships, and the agreement should say what happens if the parties disagree or separate.

Renewal risk should be tested before it becomes a service outage. Imagine that IJK pays through EGH's reseller arrangement and EGH's project ends in June. Who receives the renewal notice in November? Can IJK see the entitlements, contact support, change the reseller of record where permitted, and export its configuration? Are additional storage and log ingestion charges visible to the budget owner? The answer must be found in the purchasing and service terms, not assumed from possession of a global administrator account.

Each register entry also needs a lifecycle. Procurement records the business approval and exact SKU. Implementation records assignment, baseline configuration, acceptance tests, and evidence. Operations records health checks, usage, incidents, changes, and renewals. Transition records export, reassignment, access removal, and data disposition. A register that contains only purchase dates will not tell an incoming operator how to keep the service working.

21.19 Who owns the tenant and who owns the software

A reseller change without loss of control

Harbor Point buys its government subscriptions through a reseller introduced by EGH. At purchase, the company records the tenant identifier, verified legal customer, domains, billing contacts, primary and alternate authorized administrators, support entitlement, and subscription terms. EGH receives implementation access under its contract, and IJK receives the administration required for its managed service. The vendor retains ownership of its software and grants contractual use rights; Harbor Point controls its tenant, accounts, business data, and contractual decisions subject to

those terms. A reseller's ability to place an order should not be mistaken for ownership of Harbor Point's information or permanent control of its administrators.

Six months later the reseller proposes a new plan. The change appears modest, but the replacement might alter audit retention, endpoint features, or information protection. IJK maps every relied-on control to the old and proposed entitlement, compares the current government service descriptions and product terms, and identifies migration or configuration changes. Harbor Point's financial owner approves the purchase only after the security and business effects are understood. EGH has no automatic vote merely because it originally introduced the reseller. If EGH is still providing engineering services, it can explain a technical dependency under that agreement.

Suppose Harbor Point wants a different reseller. It should be able to identify its subscriptions, support contacts, renewal dates, and any reseller relationship or delegated permission that must change. The transition plan verifies how the vendor permits a change, ensures invoices and notices reach the right people, and checks that service is uninterrupted. It also reviews EGH's and the old reseller's access. A transfer of billing does not revoke an admin role, and removing a role does not necessarily move a license. Each relationship must be handled according to its own terms.

The same ownership questions apply to IJK's bundled services. Harbor Point may receive monitoring and backup under IJK's master agreement, while IJK is the direct customer of those vendors. The service agreement should describe what Harbor Point receives, where its data resides, what evidence it can request, the notice required before a material provider change, and how service and data transition at termination. IJK need not expose every unrelated commercial discount, but Harbor Point must understand the dependencies of its assessed environment.

A well-managed register therefore records both the legal and technical reality. It should tell a replacement administrator who may approve a subscription, who can open a support case, how a configuration can be exported, who owns the domain, where backups reside, and what happens if the provider disappears. These facts are more important to operational control than the name shown at the top of the original sales quote.

Ownership is often discussed too casually during an implementation project. The software publisher normally retains intellectual property rights in its software. The customer purchases a license or subscription under specified terms. Separately, the organization must establish control over its tenant, domains, data, administrative

identities, configuration records, and service contracts. These are related issues, but they are not the same kind of ownership.

In our example, IJK should be the identifiable customer for its own environment and should retain an authorized administrative recovery path. EGH may be the reseller and may hold delegated administration permissions, but that arrangement should not make IJK dependent on EGH's personal accounts to reach its own services. Billing contacts, domain registrations, tenant identifiers, and support relationships should be recorded in company-controlled records accessible to authorized IJK personnel.

A domain name is particularly important because control of the domain can affect email and identity recovery. The registrar account should belong to the organization under its contractual arrangements, with protected access and current recovery details. The same principle applies to certificates, application registrations, backup accounts, and automation identities. When a project engineer creates these resources, the handover must transfer practical control and documentation, not merely mention that they exist.

The right to use software lasts for the term provided by the license. A subscription normally requires continuing entitlement, while a perpetual license may permit continued use of a particular licensed version subject to its terms. A perpetual license does not necessarily include future upgrades, continuing technical support, hosted services, or security updates forever. IJK should assess the security and support life of a product independently from the word perpetual on an invoice.

Data rights, return rights, and deletion procedures should be addressed in the service agreements. IJK needs to know how it will export records, retrieve configurations, obtain retained evidence, and verify deletion when a provider leaves. These provisions should cover subcontractors and backup copies where applicable. Actual legal rights are established by the relevant agreements; an internal ownership spreadsheet cannot create rights that the contracts do not provide.

21.20 How long each party remains responsible

A timeline with overlapping duties

Before implementation, Harbor Point owns contract interpretation, information identification, scope approval, and funding. EGH owns only the discovery and design deliverables in its executed agreement. IJK continues whatever existing managed services its contract already assigns; those services do not pause because a migration

project has begun. ABC has no assessment duty before a valid engagement. This phase is vulnerable to ambiguity because sales discussions can make it appear that future providers are already responsible for current weaknesses. A dated responsibility matrix should distinguish present operator from proposed future operator.

During build, EGH may configure the tenant and deploy tools while IJK still operates the old environment. Harbor Point should designate a cutover authority who can decide when a service changes hands. An approved change record identifies who monitors each environment during the transition, where alerts go, which backup is authoritative, and who can reverse a failed step. A policy that states IJK monitors all devices is inaccurate during a pilot if only some devices have moved. The record should describe the mixed state rather than conceal it.

At acceptance, named capabilities transfer to IJK after IJK demonstrates that it can perform them. EGH remains responsible for defined defects during stabilization and for continuing obligations such as confidentiality or agreed record retention. Harbor Point retains ownership of decisions and must verify the accepted service meets business needs. If EGH finds a design defect after acceptance, the parties use the warranty or change provisions to determine correction; they do not silently assume that IJK has inherited responsibility for a defective product it never accepted.

At assessment, ABC's responsibilities arise under its authorized engagement. It may examine, interview, test, report, and perform permitted follow-up. EGH and IJK provide factual support within their contracts, while Harbor Point's leadership remains responsible for its representations and actions. ABC's completion does not renew EGH's expired stabilization agreement or shorten IJK's managed-service term. The assessment outcome is a milestone in a longer operating lifecycle.

After the assessment, the timeline continues through renewals, personnel changes, incidents, corrective work, and eventual provider transitions. IJK's duty to Harbor Point lasts through the service term and orderly termination obligations. Harbor Point's contractual duties may outlast either provider. EGH and ABC retain only the post-engagement duties defined by their agreements and governing program rules. The matrix should be revisited at each major transition so the organization does not have a week in which everyone believes someone else is monitoring a critical system.

Duration, termination, and retained obligations

ABC's assessment agreement should specify its dates, deliverables, permitted reassessment or closeout, and handling of submitted evidence. It may retain program records according to governing rules or agreement after the site visit, but it does not become Harbor Point's security operator. EGH's build contract should state acceptance and stabilization milestones and then identify residual obligations such as correction of covered defects, confidentiality, information return, and record retention. IJK's service contract should define recurring operations, support hours, notification targets, evidence delivery, renewal, and transition assistance. Harbor Point's own contractual and management accountability continues according to its DoD and customer obligations, independent of which provider is currently engaged.

Termination planning should be negotiated before a relationship becomes strained. The agreement should say how tenant administration, domains, source configuration, diagrams, runbooks, secrets, logs, backups, tickets, license records, and open issues are transferred. It should identify formats, timing, reasonable assistance, secure delivery, costs, and the treatment of provider copies. It should protect continuity without requiring the outgoing provider to keep indefinite access. IJK should be prepared to hand over Harbor Point's records and services even if Harbor Point elects another MSP, while preserving the limited business records IJK is entitled or required to retain.

For a service that depends on third-party subscriptions, the customer needs to know what changes on termination. Can the license be transferred or must a new subscription be purchased? Is the tenant controlled by Harbor Point? Can a replacement provider receive delegated administration? How long are logs and backups retrievable? Which data export is supported, and what will it cost? A contract should not promise a portability feature that the vendor does not provide. EGH and IJK should test critical exports before the first incident or provider dispute.

An annual review of provider relationships can reconcile the written terms with actual practice. A vendor may still have standing admin rights after a project closes; a support agreement may promise a response time no one is staffed to meet; a reseller may hold renewal notices without notifying Harbor Point. The review assigns corrections and captures current contacts and alternate contacts. A carefully written contract is useful only when the operational relationship still follows it.

A useful responsibility model separates continuing accountability from a time-limited service. IJK's management remains accountable for its own obligations. ABC

performs the assessment work and associated duties established by its engagement and the applicable program. EGH performs implementation, correction, and stabilization work within its statement of work. Vendors provide their services for the purchased term and under their support commitments. These periods overlap, but one does not automatically extend another.

Suppose EGH's agreement includes thirty calendar days of stabilization after written acceptance. That example should identify what happens during those thirty days. A configuration defect within the original scope may be covered, while a new customer workflow or a newly purchased application may require a change order. IJK should know who receives urgent requests, what response is promised, and whether after-hours support is included. The thirty-day period is an illustrative contract choice, not a CMMC rule.

If IJK signs a one-year managed monitoring agreement, the monitoring provider's obligations continue for that term according to the contract. The organization still needs someone to review the provider's performance, approve business-impacting actions, and maintain its internal processes. Outsourcing a monitoring task does not automatically outsource access approvals, employee training, physical safeguards, or the accuracy of an annual affirmation.

After an assessment, IJK must distinguish the assessment cycle from the maintenance cycle. The current DFARS CMMC clause describes final Level 2 status in terms of a three-year assessment period together with a current annual affirmation and continuing compliance conditions. Level 1 has an annual self-assessment cycle. The applicable contract and current program rules must be consulted for the exact status and obligations. A three-year period is not permission to leave the environment unmaintained for three years. [1]

The responsibility record should show a primary owner and a backup for each ongoing task. When one of IJK's two leaders is away, the other should be able to locate the procedures, access the appropriate systems, and contact the providers. If both are unavailable, the continuity arrangement should identify an authorized alternative. The company should test this arrangement without exposing credentials or giving unnecessarily broad permanent access to a substitute.

The contractual handoff between EGH and IJK

The implementation statement of work should divide the project into discovery, design, build, pilot, migration, acceptance, stabilization, and closure. Discovery

produces a verified information-flow and asset inventory. Design produces a decision record and responsibility map approved by IJK. Build produces repeatable configuration records rather than undocumented console clicks. Pilot uses representative users and devices, including at least one privileged workflow and one realistic recovery scenario. Migration follows an approved sequence with rollback criteria and business communications. Acceptance requires IJK to perform core operations using the delivered runbooks.

EGH should supply a design package detailed enough for another qualified operator to understand the environment. It should identify identity and administrator roles, device enrollment, endpoint policy, mail and collaboration controls, log sources and destinations, backups, network dependencies, external integrations, certificate and key custody, and service accounts. It should include an inventory of exceptions and open issues. Product screenshots may accompany the design, but they do not replace an explanation of why the settings were selected and how the configuration is validated.

Acceptance criteria should be observable. For example, the pilot user authenticates with the approved method from a managed device; a prohibited access path is denied; an administrator receives only the authorized role for the permitted period; an endpoint alert generates a case; a backup can restore a representative file with expected permissions; and a departed user loses every defined access path. The acceptance report should name the tested system, date, expected outcome, observed outcome, evidence location, and person who approved remediation or acceptance. A failed test remains in the record with its retest, so that the history is truthful.

The stabilization period should define response times, defects covered by EGH, changes that require new authorization, and the exact end date. During that period IJK should lead daily operation while EGH assists with specified corrections. If IJK cannot perform an essential procedure without EGH logging in, acceptance is premature. At closure, EGH should transfer documentation and evidence, reconcile licenses and accounts, remove unnecessary access, and obtain a written operating acceptance from IJK.

21.21 Implementing the selected environment step by step

The pilot and cutover workbooks

EGH's pilot workbook should use representative people and workflows, not only a technically skilled administrator. It includes an engineer who opens a controlled

drawing, a manager who authorizes access, an IJK technician who supports a managed device, an administrator who changes a policy, and an external collaborator who receives only approved information. Each scenario records the source and destination, identity, device, license, expected result, observed result, issue owner, and retest. Harbor Point observes whether real work remains possible; IJK observes whether it can administer and support the result.

A migration sequence begins with inventory and clean-up. Duplicate identities, stale groups, unused mailboxes, abandoned applications, and unowned file repositories are resolved or explicitly carried forward with a reason. EGH then establishes the target tenant, baseline roles, authentication, pilot policies, monitoring, backups, and a controlled method for migrating data. Sensitive data should not be copied into a temporary tool or service without review of its provider and retention. A test migration confirms file integrity, permissions, links, metadata where needed, and the user's ability to continue work. Success is measured against defined outcomes, not merely a transfer tool's completion count.

The cutover decision requires a readiness meeting. EGH presents pilot results, unresolved defects, a rollback or recovery path, and the next tasks. IJK confirms support staffing, alert routing, backup status, runbooks, and license assignments. Harbor Point confirms business timing and authorizes the interruption. The group decides what condition stops the cutover. For example, if a required identity policy fails for project engineers, the team pauses rather than bypassing the policy for every user to preserve a planned schedule. The decision and rationale are recorded.

During cutover, the team measures what happened. It validates mail flow, sign-ins, access to the controlled repository, external collaboration where approved, endpoint and log reporting, backup jobs, and help desk routes. Users receive a concise explanation of what changed and where to report a problem. A failed test is assigned and retested. EGH does not close the migration simply because the last data copy ended; IJK does not accept an environment without the procedures and access it needs to operate it.

After the change, source-system shutdown needs its own plan. Old accounts, permissions, stored copies, connectors, and backup sets may still contain regulated data or provide access. Harbor Point determines retention and disposition requirements, IJK verifies operating evidence and monitoring in the new environment, and EGH removes temporary tooling and privileges. A controlled cutover includes the cleanup, not just the launch announcement.

Implementation begins with approved prerequisites. IJK confirms the scope, budget, service selection, information handling rules, and authorized contacts. EGH confirms eligibility and purchasing requirements with the appropriate provider, obtains the necessary subscriptions, and establishes the target environment. The project records the tenant identifiers, domain plan, approved administrative accounts, and recovery arrangements before ordinary business information is introduced.

The next stage establishes identity and access. EGH creates the required account structure, assigns limited roles, configures approved authentication methods, and tests recovery. IJK supplies an approved user roster and access decisions. Group membership should reflect real business roles, such as controlled-project personnel or authorized administrators. Copying all existing accounts into every new group simply preserves old access problems in a newer platform.

Device preparation follows the identity foundation. EGH enrolls pilot devices, applies configuration policies, enables required protection, and checks reporting. The pilot should represent ordinary work rather than only the engineer's test laptop. IJK should include a user who performs the controlled project workflow and an administrator who will maintain the system. Their experience will reveal problems with file access, application compatibility, printing, or remote work before the entire organization is affected.

The collaboration and information handling configuration should then be tested with non-sensitive sample material. EGH creates the approved workspaces, configures access and sharing, and demonstrates both authorized and prohibited actions. IJK confirms that employees can perform their work without using personal email or unsupported file-sharing tools. If a business process cannot function under the proposed controls, the design must be revised and approved before migration.

Logging, backup, and response capabilities should be operational before production migration is accepted. The parties generate test events, retrieve the resulting records, restore sample data, and exercise alert escalation. This sequence prevents the organization from moving important information into an environment whose protection cannot yet be observed or recovered. It also creates baseline evidence that later administrators can use when troubleshooting changes.

Migration should occur under a written change plan. The plan identifies the source data, authorized migration accounts, transfer tools, temporary storage, validation method, rollback decision, and disposition of residual copies. During cutover, IJK communicates expected user actions and available support. Afterward, EGH and IJK

reconcile migrated content, permissions, subscriptions, and integrations against the plan, then investigate omissions before declaring completion.

21.22 Testing and accepting the implementation

A defect log with consequences

Every acceptance test should have an expected result and an observed result. Suppose a prohibited unmanaged laptop reaches the protected repository. EGH records the device and account used, time, path, and policy result, then investigates whether the device was misclassified or a conditional access rule was scoped too narrowly. IJK checks whether similar devices exist. Harbor Point decides whether the finding blocks acceptance because its business and security implications are clear. The defect remains open until the policy is corrected and a negative test proves denial on representative devices.

Some tests appear successful until the evidence is examined. An endpoint alert might show in the vendor console but never create an IJK ticket because the connector lacks a license or token. A backup might restore a file but grant access to a wider group than the source. A departing user's account might be disabled while a separate application session remains active. These cases show why a test needs a business outcome, a technical mechanism, and an evidence trail. The acceptance team should examine the complete chain rather than collecting unrelated green screenshots.

The defect log distinguishes severity and treatment. A typographical error in a runbook can be corrected before closure without delaying all work; an absent log source relied on for detection may block operating acceptance. Each defect has an owner, business effect, interim treatment, target date, validation method, and decision authority. Harbor Point can accept residual issues only within applicable contractual and security requirements. An internal waiver cannot make an unimplemented external requirement implemented.

Retesting should be performed by someone other than the person who made the correction where practicable. IJK needs the confidence to repeat the operation after EGH leaves, so it should lead selected retests. Harbor Point's owner observes business-critical scenarios, and EGH supplies the configuration details. The record preserves the original failed result and the later pass. This makes the evidence credible and helps the team find the same root cause in other parts of the environment.

At final acceptance, the parties sign or otherwise approve a record listing delivered components, tests, documentation, licenses, open defects, stabilization period, and the point at which routine operation transfers to IJK. The record should be understandable months later to someone who did not attend the project meeting. ABC may later examine some of these artifacts, but acceptance remains Harbor Point's decision about the implementation it purchased.

Acceptance tests mapped to business consequences

The test plan should be written before EGH considers the project complete. Each test names the underlying business or security outcome, the environment and population, the operator, the expected result, and the evidence that will be retained. A login test asks whether the right engineer can reach the right project from an approved device while an unauthorized user cannot. A logging test asks whether a privileged action is visible to the people who must investigate it. A restore test asks whether the correct data and permissions can be recovered within the approved objectives. These outcomes are more meaningful than checking whether a product dashboard displays an enabled setting.

The plan should include negative tests. An unapproved device should fail to reach the controlled workspace. An ordinary help desk technician should be unable to grant itself unrestricted privilege. A former employee should be unable to use an existing browser session or mobile token after offboarding. An external sharing request should follow the approved decision route rather than succeeding through a default link. A negative result that unexpectedly succeeds is a finding. The team records the failure, corrects the configuration or process, and repeats the test without deleting the first observation.

Tests also need a service-provider dimension. EGH demonstrates that IJK can receive alerts and administer the environment after handover. IJK demonstrates to Harbor Point that it can retrieve evidence and explain an incident escalation. Harbor Point demonstrates that it can identify an authorized approver for new access and an official for contractual decisions. A polished demonstration by EGH alone can conceal missing operational ownership. The final acceptance decision should explicitly list tests passed, unresolved defects, their implications, and the approved next action.

Acceptance should not be equated with assessment success. ABC may later sample different personnel, devices, records, and time periods. The internal test establishes a

reliable starting point; IJK's subsequent ordinary records show whether it remains true. Harbor Point should schedule operating reviews after acceptance and retain the original design rationale so later changes can be judged against the intended protected workflow.

Acceptance tests should demonstrate results that matter to the organization. A successful sign-in test proves that an authorized user can work under the intended conditions. A denied-access test proves that an unauthorized identity or unsuitable device cannot perform the same protected action. A log test proves that the relevant event is recorded and retrievable. Together, these tests provide stronger evidence than a collection of screenshots showing that settings were selected.

For example, EGH can create a sample document in the controlled project workspace. An authorized pilot user opens it from a managed device. A user outside the approved group attempts access and is denied. The team then confirms whether the events expected under its logging design are available for review. The test uses harmless sample content and records the identities, devices, time, expected results, actual results, and any corrective work.

Backup acceptance should include recovery by IJK personnel following the written procedure. If only EGH's engineer knows which hidden account or undocumented setting is required, the handover is incomplete. The same principle applies to a lost authentication device, an endpoint alert, an employee departure, and a failed patch deployment. IJK should be able to perform representative tasks without improvising or relying on the installer's memory.

A defect register should separate items that prevent acceptance from items that can be resolved through an explicitly approved plan. It should identify the affected requirement or workflow, owner, corrective action, due date, and retest result. The register should not disguise an unmet security requirement as a cosmetic issue. IJK should understand the assessment consequences of outstanding work before accepting a production milestone.

The acceptance record should reference the tested configuration baseline and the exact deliverables received. It should also state the beginning of any stabilization period and the remaining access granted to EGH. Written acceptance is evidence of a project decision; it is not an assessment result. ABC must still perform its independent work when the required assessment is undertaken.

An acceptance meeting that tests actual operation

At the acceptance meeting, EGH should not simply announce that configuration is complete. An IJK operator who was not the primary installer should demonstrate ordinary tasks from the runbook: add an approved engineer, enroll a replacement laptop, locate the device in endpoint protection, investigate a suspicious sign-in, retrieve a relevant audit record, and restore a file. Harbor Point's owner or authorized manager observes the tasks against the approved business requirements. The result exposes missing permissions, instructions, or supporting entitlements while EGH remains contractually available to correct them.

The meeting also tests exceptions. What happens when an engineer needs temporary external collaboration? Who decides whether a drawing can be shared, and which tool is approved? What if a laptop cannot enroll because an application requires an older operating system? What if a backup job succeeds but the restored file is inaccessible? EGH describes the technical options and constraints; IJK explains the operating workflow; Harbor Point authorizes business changes and the disposition of regulated information. Any unresolved issue is recorded with its owner, target, interim treatment, and effect on acceptance.

Handover should be an inventory of usable assets, not a stack of files. It includes design decisions, diagrams, system security plan inputs, license and vendor register, administrator and service-account inventory, exported configurations, monitoring and backup coverage, known exceptions, change history, open tickets, test results, support contacts, and evidence locations. Each item needs an owner and a currency date. Secrets move through a secure vault under Harbor Point or IJK control, with access review and rotation where appropriate. A shared spreadsheet containing passwords would undermine the point of the handoff.

The written acceptance separates accepted functions from remaining obligations. EGH might have thirty days to repair a defective log connector, while IJK assumes daily monitoring once the alert path works. Harbor Point should not mark the entire environment accepted if an essential control has never been demonstrated, and EGH should not be held indefinitely for new business requests outside its statement of work. A clear acceptance record protects all three parties because it states what was tested, what remains open, and when support ends.

21.23 Transferring knowledge and limiting installer access

A transfer test led by the new operator

EGH presents a runbook to an IJK technician who did not build the tenant. The technician receives an approved onboarding request and follows the written steps while EGH observes silently. If the procedure omits a license assignment, device group, or verification step, the omission is corrected immediately. The technician then retrieves a suspicious sign-in, identifies the log source, opens a case, and explains when Harbor Point should be notified. This exercise exposes assumptions that an installation team may never write down because its members remember them.

The handover package includes architecture diagrams, tenant and domain identifiers, administrator and service-account register, licenses and renewal terms, endpoint groups, policy exports, log and alert mapping, backup and restore procedures, change history, open defects, provider support paths, and evidence locations. Each artifact has an owner and date. IJK checks whether it can find and use the records, and Harbor Point ensures the company retains access even if its MSP relationship changes. The package should describe how to maintain and recover the design, not only how it was installed.

Secrets move through a controlled vault or equivalent process. EGH should not leave passwords in a design diagram, unencrypted spreadsheet, chat history, or recorded demonstration. IJK verifies the service-account dependencies before rotation so that a cleanup action does not stop logging, backup, or migration reconciliation. Installer roles, API grants, certificates, delegated relationships, and support identities are inventoried separately from secrets. Each receives a disposition: revoke, rotate, transfer, restrict during stabilization, or retain under a newly authorized service contract.

The operating team performs a recovery drill after EGH's routine access is removed. It tests vendor support contact, emergency identity access, evidence retrieval, backup restoration, and a representative configuration change. A deficiency is not hidden merely to complete the project. EGH fixes a covered defect under its terms, IJK updates the runbook, and Harbor Point decides whether the handover is complete. The drill gives management practical assurance that the company can operate the environment without the original implementer's personal account.

Knowledge transfer is not a one-hour presentation. It includes written material, practice, questions, correction, and a second operator who can repeat the task. IJK

should train its alternate and place recurring work on a calendar. Harbor Point should understand which decisions remain its own. ABC's later interviews can then reach people who actually perform the work rather than a consultant who remembers the installation story.

A complete handover contains operational explanations as well as technical records. IJK needs an architecture description, asset and software registers, role assignments, configuration baselines, support contacts, subscription details, recovery procedures, and the location of evidence. The documentation should explain why important settings were chosen. Without that reasoning, a future administrator may remove a restriction that appears inconvenient without understanding the requirement it supports.

Training should use actual operating scenarios. EGH can demonstrate a procedure, then observe an IJK administrator repeat it using the written instructions. The exercise should reveal missing steps, unclear decisions, and dependencies on the installer's credentials. IJK should update the procedure while the engineer is available to answer questions. A recorded presentation may be useful, but it is not a substitute for demonstrated operating capability.

Credentials should be transferred through the approved secrets management process. They should not appear in the ordinary handover document, an email attachment, or a meeting recording. IJK should rotate or otherwise secure relevant secrets after transition according to the design, particularly where multiple project personnel had access. Service account dependencies must be understood before changing credentials so that cleanup does not silently stop backups or automation.

EGH's privileges should be reviewed account by account. Access still needed during stabilization should have a documented purpose, limited scope, and scheduled expiration or review. Access no longer needed should be removed, including delegated relationships, application permissions, tokens, remote agents, and unmanaged credentials. Removing one named account does not prove that every installer access path has been closed.

IJK should retain evidence of the access review and confirm that ordinary operations still function afterward. If a provider's ongoing service depends on continuing access, that access belongs in the ongoing service agreement and operating records. It should not survive merely because no one remembered to remove it when the project ended.

Operating the cloud and security tools after handover

Daily work starts with service and control health. The assigned IJK operator checks whether the identity service is reachable, privileged sign-in alerts are investigated, managed devices are reporting, endpoint protection is healthy, required logs are arriving, backups have completed, and high-priority tickets are owned. This is not a command to stare at every console throughout the day. The team should use monitored alerts and a defined exception queue, then record the investigation and action when a signal indicates a problem. A green dashboard without a known covered population is weak assurance.

A weekly review reconciles the assets and accounts that should exist with those that appear in the operating tools. IJK compares the approved user list to active identities, the device register to endpoint management and detection coverage, and the log-source register to actual ingestion. A laptop absent from protection is investigated even if no malware alert appears, because the absence itself is the problem. The reviewer records missing coverage, reason, owner, target date, and independent validation of correction. Repeated failures should prompt a process change, not only one manual fix.

The same cadence applies to change and patch work, but urgency follows actual exposure and the company's approved process. IJK evaluates vendor notices, authenticated scan findings, known exploitation, affected assets, dependencies, and available mitigations. It schedules testing and deployment, preserves change approval, verifies installation, and checks that the vulnerability has been addressed. If a server cannot be patched immediately, the team documents its interim treatment and the person authorized to make the business decision, while recognizing that internal acceptance does not waive an external requirement.

Backup maintenance deserves an independent check. Successful job logs show that data was copied, while a restore exercise shows whether a usable result can be recovered. IJK should periodically restore representative records and a more demanding workload according to its recovery objectives, confirm access permissions and application function, and record lessons from failures. It should know who can initiate restoration, where keys are held, how an unavailable provider would be replaced, and how it would preserve relevant evidence after an incident.

21.24 Daily and weekly maintenance

A week of ordinary operations

On Monday morning IJK checks that the overnight backups completed, required log sources are reporting, endpoint agents are healthy, and critical alerts have an assigned analyst. The operator compares expected populations with observed results. If a device disappears, a log connector stops, or a backup fails, the operator creates an exception record and follows an escalation based on the service's importance. A status dashboard is a useful starting screen, but it does not establish that every expected system is present. The service inventory supplies the denominator against which tool health is interpreted.

On Tuesday an engineer requests access to a new project folder. The technician confirms an authorized approver, grants the narrow group membership, tests the user's access, and records the change. On Wednesday a different engineer leaves the company. The offboarding process revokes access, sessions, and relevant application permissions, addresses the device, and validates the result. These routine tickets become evidence that identity processes operate. A quick phone request may feel efficient, but without an approval and execution record the organization cannot reliably show who made the decision or whether every access path was removed.

Thursday is scheduled for patch and vulnerability review. IJK examines newly reported findings, validates affected assets, prioritizes work based on the approved risk process, and plans changes that might disrupt engineering software. Harbor Point approves an outage window when needed. The team tests representative devices, deploys approved fixes, and verifies results. When an update fails, the record describes why, what interim measure is in place, and when the next attempt will occur. The operator also checks whether a previously closed finding has recurred because a device was rebuilt from an old image.

Friday's review reconciles inventories. The asset list, management console, endpoint platform, vulnerability scanner, backup coverage, and user directory will not always display identical counts, so IJK explains differences rather than forcing each report to match. One spare laptop may be powered off; another device may have been retired without removing its agent. The review names actual exceptions and corrective actions. It also checks unresolved alerts and open change requests before the weekend, with an alternate contact assigned for after-hours incidents.

The week's records feed management reporting without requiring a separate evidence-creation exercise. Tickets show approvals and changes, tool reports show technical state, exception records show detection and correction, and meeting notes show decisions. IJK should protect those records because they reveal system details and sometimes contain regulated information. Harbor Point's managers need a concise view of meaningful exceptions, while ABC later receives relevant samples only through its assessment process. The purpose of routine work is protection; useful assessment evidence is a disciplined by-product.

A daily operating review should focus on time-sensitive failures and events. Depending on the environment and staffing model, this may include significant security alerts, failed backups, unavailable logging sources, newly discovered critical exposure, and suspicious privileged activity. The review should identify who examined the information, what required action, and where the action was recorded. A dashboard opened without follow-up is not the same as a functioning review process.

The organization should define what happens when the designated reviewer is absent. In our two-leader example, one person performs the routine review while the other receives escalations and can assume coverage. A managed provider may supplement this arrangement, but IJK should know which events the provider actually monitors. Alerts outside the purchased service should not be assumed to receive attention simply because a monitoring contract exists.

Weekly maintenance can examine trends and exceptions that do not require immediate action. IJK might review devices that have not reported, patch deployment failures, unresolved vulnerability findings, privileged changes, and repeated user problems. These reviews should result in decisions. A device that repeatedly fails updates may need repair or replacement, while a recurring authentication problem may reveal a training or enrollment issue.

A useful operating record connects the observation to the resolution. For example, the weekly review identifies a laptop that has missed its management check-in. A ticket records contact with the employee, diagnosis of the failed service, repair, and confirmation that the device is again reporting. The record gives an assessor or manager a way to understand the actual process without requiring the employee to remember the event months later.

Daily and weekly frequencies are examples for an operating plan. IJK should set its actual cadence according to requirements, risks, workload, and response

commitments. The cadence must also be realistic. A written promise to review every event every hour is harmful if the company has neither the staffing nor the automation to perform it and cannot show that it does so.

21.25 Monthly quarterly and annual maintenance

A year of reviews and a material change

In January Harbor Point and IJK approve an operating calendar. Monthly reviews examine access changes, tool coverage, incident trends, backup restoration, vulnerabilities, license and capacity warnings, and new data flows. A quarterly meeting samples selected records and challenges whether the written procedures still match what technicians do. The annual review addresses assessment status, affirmations where applicable, provider agreements, budget, recovery strategy, and the complete system security plan. These frequencies are an internal example unless a contract or other applicable requirement specifies otherwise. The calendar should name an owner and alternate rather than merely a recurrence in one person's inbox.

In March Harbor Point wins a contract that introduces a different information type and an external design partner. The next monthly meeting is too late to begin analysis if the work starts immediately. The program manager triggers a change review, the data owner clarifies handling, EGH or another engineer evaluates the collaboration architecture under an active agreement, and IJK checks identity, device, logs, backup, and support implications. Harbor Point decides whether the existing assessed boundary and service commitments can support the new work. The decision and test results update the scope documentation before ordinary users begin moving material.

In June a quarterly sample shows that offboarding tickets close promptly but a third-party application retains sessions for several departed users. IJK identifies the root cause in the procedure and checks all recent departures, not just the sampled employee. Harbor Point approves the correction and any necessary incident analysis. The process is revised so future offboarding includes application-session revocation and validation. The review record preserves the finding and subsequent correction. A reviewer should see a functioning feedback loop rather than a perfect-looking history created by deleting exceptions.

In September a license renewal proposes a lower-priced plan. The security lead maps features used by the environment, identifies any rights the proposed plan removes, and tests an alternative design if management wants the savings. The budget owner sees the total annual cost, including added storage and log volume. No one assumes

that a product name will remain equivalent after a vendor changes packaging. The decision record is attached to the register, and monitoring verifies continuity after renewal.

At the annual review, Harbor Point's affirming official should receive a current account of the system's scope, material changes, open deficiencies, assessment status, and operation. IJK prepares technical evidence and identifies uncertainty; leadership decides whether the statement can be made under the applicable rules. ABC is engaged only if the assessment pathway or new independent work calls for it. The annual meeting is not an excuse to postpone known issues until the next anniversary. Event-driven reviews throughout the year keep the program aligned with reality.

Review cycles with a reason for each interval

A monthly management review is useful because subscription, staffing, device, and incident conditions can change before an annual assessment date. IJK brings scope changes, open security findings, control-health exceptions, license and renewal issues, backup test outcomes, incident lessons, and evidence gaps. Harbor Point's accountable manager asks what changed, what remains unresolved, what decision is needed, and whether the system security plan still describes the environment. The minutes name owners and due dates. Monthly is an example internal cadence, not an invented CMMC requirement for every control.

A quarterly review can challenge assumptions that daily operators might stop noticing. A second person samples recent access approvals, privileged actions, closed vulnerabilities, restore results, and provider notifications. The team looks for exceptions that repeat, unowned service accounts, dormant delegated access, and integrations added without scope analysis. It checks the responsibility matrix against the real people performing work. If IJK repeatedly handles a task that the contract assigns to Harbor Point, the parties update the agreement or fix the practice rather than letting the mismatch become normal.

The annual cycle examines the program as a whole and connects it to applicable affirmations, contract renewals, and assessment planning. Harbor Point confirms its current contracts and required status, reviews the defined scope and system security plan, examines material changes and unresolved issues, and ensures the affirming official has a supportable basis for any required statement. IJK renews training and alternate coverage, reviews disaster recovery and provider transition, and budgets for technology replacement. EGH participates only if it has an active agreement. ABC

performs an assessment only under a valid engagement and applicable independence rules.

No fixed calendar can replace event-driven review. A major incident, new CUI flow, customer acquisition, tenant migration, switch of backup provider, loss of a critical administrator, or revised contract clause can require immediate analysis between scheduled meetings. The maintenance plan should define who recognizes such triggers, who approves changes, how scope and evidence are updated, and how relevant customers or authorities are informed.

Monthly review should connect technical performance with management decisions. IJK can examine unresolved risks, service availability, access changes, recurring incidents, backup test results, license consumption, and approaching renewals. The report should explain material exceptions and the resources needed to correct them. Leadership needs a clear account of what requires a decision, rather than a large export of security events with no interpretation.

Quarterly activities may include a broader access review, a review of external providers, selected recovery exercises, and validation of important configuration baselines. The appropriate frequency depends on the organization's obligations and policies. The review should include administrators and non-human identities as well as employees. An application registration with broad permissions can remain powerful long after its original business sponsor has left.

Annual work includes reviewing the program as a whole and completing applicable assessment and affirmation obligations. IJK should examine whether the scope, system security plan, incident procedures, training, contracts, and operating resources still match reality. It should verify that significant changes have been incorporated into the evidence and that the authorized official has a defensible basis for any required affirmation. The affirmation should be the result of review, not an automatic calendar response. [1]

Renewals should be scheduled far enough ahead to allow technical and financial review. IJK should examine user counts, unused subscriptions, server coverage, storage growth, support commitments, and changes in product rights. A lower-priced renewal may remove a feature on which a control depends. A higher-priced bundle may provide no useful benefit if the added features are unavailable in the government environment or will not be operated.

The annual operating plan should budget for human effort as well as licenses. Training, evidence maintenance, incident exercises, recovery testing, provider review, and independent assessment preparation require time. The organization should also reserve resources for replacement equipment and unexpected remediation. A design that consumes the entire budget on subscriptions leaves no capacity to maintain the protections those subscriptions were intended to support.

A reporting packet that leads to decisions

IJK can use a single monthly packet with several layers. The opening narrative explains material changes to the protected boundary, notable incidents, important exceptions, and decisions needed from leadership. A technical annex contains the covered population and control-health detail behind those conclusions. A corrective-action register connects each unresolved issue to a responsible person, due date, interim treatment, validation method, and management escalation point. The packet should state when a metric was measured and which systems were included, so a reader can reproduce or challenge it.

For an eight-user controlled workload, a report that says all users have multifactor authentication may conceal a privileged service account or emergency access path outside the ordinary user list. The report should describe the population: eight users, two named administrators, any approved service identities, and each exception with its reason and compensating procedure where appropriate. The source might be an identity export and a sign-in policy review, while a sampled authentication test checks whether the intended enforcement actually operates. The same principle applies to device coverage, backup success, vulnerability closure, and log availability.

The three parties receive different reports. EGH receives a defect list and limited evidence needed during its contractual stabilization period. ABC receives assessment evidence through the agreed assessment process, with any later closeout materials subject to that process; it is not the standing recipient of IJK's operational dashboard. IJK's management receives the operating packet and approves spending, remediation priorities, and external representations. A customer receives only the service, incident, and evidence reports specified in its agreement and permitted by information-handling rules.

A monthly meeting should result in recorded decisions rather than a collection of charts. If a logging service is nearing its licensed ingestion threshold, management decides whether to fund capacity, change the architecture, or take another compliant

action. If a provider repeatedly misses its notification target, management decides how the contract and escalation process will be corrected. The minutes should identify the decision, rationale, responsible owner, date for follow-up, and supporting record.

21.26 Internal reporting and management decisions

A management meeting that changes the plan

The monthly packet reaches Harbor Point's leaders before the meeting. Its first page states the protected population, changes since the last review, significant events, unresolved exceptions, and requested decisions. A technical annex gives source reports and definitions. IJK presents one missing endpoint agent, a successful restoration test after an earlier permissions failure, an overdue application owner review, and a log-capacity forecast. The leaders should be able to ask what each fact means for the business, how it was measured, and what must happen next. A packet that only reproduces vendor graphics cannot answer those questions.

The missing agent affects an engineer's laptop. IJK has isolated the cause to a failed enrollment step and corrected the device, but its check of other rebuilds is still underway. The report does not say all devices were protected for the month. It states the gap interval and what is known, identifies the owner of the population check, and sets a validation date. Harbor Point's leader asks whether project work occurred on the device and whether additional analysis is needed. The resulting decision and rationale become part of the issue record.

The log-capacity forecast requires funding. IJK explains the current ingestion rate, expected growth from two new servers, capacity limit, likely effect of crossing it, and available vendor options. Harbor Point can authorize an increase, request a technically valid redesign, or defer the servers until the architecture is ready. The minutes state the selected path and deadline. They do not merely say leadership was informed. A security report has value when it enables a timely decision that preserves the control.

The packet should separate the audience. The technician receives alert and query detail. IJK's operating manager receives trends and service failures. Harbor Point's executives receive business consequences, contractual exposure, spending choices, and overdue action. A customer service report may have different terms and restricted content. ABC receives selected evidence under its assessment engagement. An

incident notice follows its own urgent route rather than waiting for the next packet. Distribution rules protect system details while ensuring accountable people can act.

At the following meeting, the first question is whether the previous decisions worked. IJK shows that the agent comparison now catches rebuilt laptops, that log capacity has been increased before reaching the limit, and that the application owner completed the access review. Any item still open retains an owner and escalation. This continuity turns monthly reporting into management of a live program rather than a ceremony in which each month's slides are forgotten.

Three audiences for the same evidence

A technical case record for a missing endpoint agent includes device ID, last telemetry, enrollment state, logs, diagnosis, commands run, and retest. The operating manager needs the affected population, gap interval, root cause, similar devices checked, and service performance. Harbor Point's executive needs the business exposure, contractual implications if any, spending or schedule decision, and date of closure. These are three views of one underlying event. IJK should preserve the authoritative case and create summaries suited to each audience without changing the facts between versions.

A monthly packet can contain a one-page narrative and a compact supporting register. The narrative identifies material changes and decisions. The register names each open issue, owner, next action, due date, evidence source, and escalation status. Trend measures such as device coverage or overdue vulnerabilities are useful when the denominator and measurement date are shown. A hundred-percent figure without a complete asset list is weaker than a lower figure accompanied by named exceptions and a credible correction plan.

Customer reporting follows the service agreement. Harbor Point may expect prompt notice of a high-severity alert, a weekly exception summary, and a monthly management meeting. Another customer may have different terms. IJK should avoid sending one customer's sensitive evidence to another or using a cross-customer dashboard as a substitute for tenant-specific facts. ABC receives evidence only through its independent engagement, and EGH receives only the information necessary to correct a covered installation problem. The distribution list is part of information protection.

Reports should lead to decisions and then be checked. If Harbor Point authorizes additional log capacity, the next packet confirms purchase, activation, observed

ingestion, and new threshold. If it declines a proposed service, the record explains the approved alternative and its validation. An issue should not vanish from the packet solely because its owner missed a deadline. Management's recorded review is evidence that leadership governs the program, but the technical evidence must still support the underlying claims.

Sample narrative from a monthly management report

A useful report might begin as follows: During September, Harbor Point added two engineering users and retired one controlled-workload laptop. IJK confirmed both new users had approved access and compliant managed devices before they entered the project workspace. The retired laptop was removed from identity, management, and endpoint inventories and its storage was processed under the approved disposal procedure. This statement is supported by named tickets and inventory records. It gives management a factual view of change rather than a count of help desk closures.

The next paragraph might address a problem: The backup job for the engineering file repository completed on schedule, but the September restore exercise found that restored permissions were too broad. IJK restricted the test copy, corrected the recovery procedure, and repeated the restore. The follow-up test succeeded on September 18. Harbor Point's manager approved the revised procedure, and the original failed result remains in the evidence record. This is an honest account of a detected control weakness and its resolution. A report that says only one hundred percent backup success would conceal the important finding.

A decision request should then be explicit: Security log ingestion is forecast to exceed the purchased capacity in October because two additional servers were added. IJK recommends purchasing the documented additional capacity or approving an architecture change that retains the required event sources. Management must decide by the vendor's renewal deadline to avoid dropped telemetry. The report names the cost source, affected services, alternatives, decision owner, and due date. A graph without the decision would not prevent a control failure.

The final part should connect to contractual status without overclaiming. Harbor Point's affirming official is due to review current status and supporting evidence on a specified date; the operating team has identified one open exception and is investigating whether it affects the statement. The report should not preapprove an affirmation. It should give the official the facts and a route to resolve uncertainty.

ABC does not need this routine management report unless its independent engagement requires relevant evidence.

Reporting should have a defined audience and purpose. The technician needs enough detail to investigate an event. The operating manager needs to know whether services and controls are functioning. Senior leadership needs to understand significant exposure, overdue corrective work, required expenditures, and decisions affecting contracts. These audiences may use the same underlying records, but they should not all receive an identical unfiltered report.

For IJK, a monthly management report can begin with changes in scope and important operating events. It can explain that two employees joined the controlled project, one device required replacement, one backup test exposed a permissions issue, and an upcoming renewal requires a funding decision. Each statement should connect to a record or action. The report should distinguish resolved issues from unresolved ones and identify the person responsible for follow-up.

Metrics need a defined population and calculation. A statement that ninety-eight percent of devices are protected is difficult to interpret if the inventory is incomplete or servers are excluded without explanation. A more useful report identifies the covered population, the devices missing protection, the reason for each exception, and the corrective deadline. Management should be able to understand the practical consequence of the gap.

ABC does not automatically need every monthly report after an assessment, and EGH does not automatically retain access to all operating records after installation. Distribution should follow the engagement, information sensitivity, and recipient's need to know. IJK should agree in advance on any reports required by customers, insurers, subcontract agreements, or other obligations. Routine distribution should use an approved channel appropriate for the information included.

Reports containing sensitive system details deserve protection. An inventory, vulnerability export, or incident summary can reveal useful information to an attacker even when it contains no project document. IJK should apply its approved handling rules, limit recipients, and maintain appropriate access and retention. The purpose of reporting is to support action and accountability without creating unnecessary disclosure.

21.27 CMMC status and affirmation reporting

A truthful annual affirmation process

The process begins months before the affirmation is due. Harbor Point identifies every CMMC UID and associated contractor information system relevant to its contracts, the applicable assessment status and date, and the affirming official. It confirms the current clause and submission instructions rather than relying on an old calendar entry. IJK maintains a change record showing new users, devices, applications, providers, locations, incidents, and unresolved control gaps. Harbor Point compares those changes to the scope and system security plan represented by the current status. EGH may supply information about its former installation but does not decide what Harbor Point may affirm.

A preparation meeting examines evidence by control family and operating process. The team samples access approval and review, managed device coverage, vulnerability handling, logging, backup, incident readiness, personnel procedures, and provider services relevant to the boundary. It asks whether records show routine operation across the period and whether exceptions were corrected or remain open. The packet includes the current SSP and known issues; it should not suppress a failed restore or a temporary monitoring gap. The authorized official needs an accurate picture, including uncertainty, before signing a statement about continuing compliance.

If an unresolved issue may affect the ability to affirm, Harbor Point consults the applicable rule, contract, and qualified advice as needed and determines corrective and reporting actions. IJK can provide technical facts and a remediation proposal. It cannot waive a requirement by labeling the issue accepted risk. A conditional status or POA&M path is available only where the governing rules allow it and under the relevant time limits and closeout process. A routine project backlog is not a substitute for an assessment-defined POA&M. [1]

The submission record preserves the identity and authority of the official, the system and UID, the status and evidence reviewed, the date, channel, confirmation, and any subsequent correction. If a contracting officer or prime requires information under the clause or subcontract, Harbor Point sends the specific information through the appropriate channel and records the transmission. The technical team should not email a vague claim of certification in place of the required identifiers and current

status. Customers supported by IJK may have their own separate status and official; IJK's internal affirmation does not automatically cover them.

The day after affirmation, the program continues. IJK monitors controls and scope changes, Harbor Point funds corrective work, and the calendar schedules the next review. If a new contract changes the boundary, management evaluates it immediately. The annual date is a required checkpoint under applicable terms, not a permission to let the environment drift for the rest of the year.

Who prepares, who decides, and who submits

The reporting process should begin with a contract register. For each covered contract or subcontract, Harbor Point records the relevant clause, required CMMC level and assessment path, systems that perform the work, CMMC UID where applicable, status date, affirmation date, and contractual points of contact. IJK may maintain the technical mapping and evidence calendar, but Harbor Point's authorized personnel validate the contractual interpretation. When a new task order changes the information received, the team checks whether the existing scope and status still cover that work before making a representation to the prime or contracting officer. [1]

The evidence packet for an annual affirmation should be prepared before the deadline. IJK provides operating records: access reviews, privileged-role changes, device coverage, vulnerability and patch history, log health, backup tests, incident records, provider changes, and open issues relevant to the assessed boundary. Harbor Point's managers compare those records with the current system security plan, approved scope, and prior assessment. A designated affirming official decides whether the required statement can truthfully be made. A reminder email, an unqualified dashboard percentage, or the fact that a past assessment succeeded is not a sufficient basis.

Where a valid conditional status and POA&M closeout path applies, its deadline and eligible items must be tracked separately from routine remediation. The owner records the exact assessment finding, authorized remediation, milestones, evidence of implementation, validation, and required submission or closeout procedure. IJK can perform technical work, EGH can assist under contract, and ABC or the applicable assessment body performs only the role authorized by the program. A customer should not present a general backlog of wished-for improvements as though every item qualifies for conditional treatment. [1]

Reporting confirmation is evidence too. The register should capture who entered or affirmed information in SPRS, when, for which system and UID, the confirmation obtained, and what information was sent to a contracting officer or prime as required. If a correction is needed, Harbor Point records the original submission, reason for correction, authorized decision, and revised confirmation. Distribution is limited to those who need the information. The aim is a traceable organizational statement, not a private technician's assertion that the company is certified.

CMMC status reporting is separate from ordinary operational reporting. The applicable contract identifies the required level and assessment type. A self-assessment is not interchangeable with a required C3PAO assessment, and a supplier's statement that it is CMMC ready is not equivalent to the required status. IJK should verify the actual contractual requirement before deciding which assessment and reporting process applies.

DFARS 252.204-7021 requires the contractor to maintain the applicable current CMMC status for relevant systems throughout contract performance when the clause applies. It also addresses annual affirmations in the Supplier Performance Risk System, or SPRS. The clause calls for providing applicable CMMC unique identifiers to the contracting officer and reporting changes in those identifiers. IJK should track the identifiers against the actual systems and contracts they support. [1]

For assessments that require self-assessment reporting, the contractor must ensure that the required results are entered through the prescribed process. Independent assessment results follow the applicable assessment process, while the organization's authorized affirming official has its own responsibility for continuous-compliance affirmation. IJK should identify who prepares supporting material, who reviews it, who is authorized to submit it, and how submission evidence is preserved.

The annual affirmation requires a management review of the continuing basis for compliance. Before submission, IJK should examine material changes, unresolved failures, applicable assessment status, and the evidence supporting current operation. A previous successful assessment does not excuse an inaccurate present statement. If a significant issue arises, management should determine the required corrective, contractual, and program actions instead of treating the anniversary date as a reason to make an unsupported affirmation.

Conditional status requires particular attention. The current clause describes conditional Level 2 status within a period not older than 180 days and requires successful closeout of a valid plan of action and milestones to achieve final status.

The detailed eligibility and closeout rules must also be applied. A general project task list is not automatically an allowable CMMC POA&M, and the organization should not assume that every unmet requirement can be deferred. [1]

IJK should keep a reporting calendar that separates assessment dates, affirmation dates, conditional closeout deadlines where applicable, and contract-specific submissions. It should assign a primary and backup owner and set internal preparation dates before each external deadline. The calendar should be updated when contracts, assessment identifiers, or status change. This reduces the risk that a technically maintained environment develops a contractual problem because required reporting was overlooked.

21.28 Cyber incident reporting and evidence preservation

The first seventy-two hours as a decision timeline

At 9:10 a.m. IJK receives an alert that a privileged account accessed Harbor Point's protected project site from an unexpected location. The analyst records the source, time, account, device, and initial uncertainty. By 9:25 a.m. the on-call lead has reviewed recent sign-ins and opened an incident case. The team may revoke sessions or disable an account under its authorized containment procedure while preserving the original records. Harbor Point's incident lead receives an early notification with known facts and an explanation of what is still being checked. Early notice matters because a provider's internal investigation does not suspend the contractor's reporting obligations.

Harbor Point evaluates whether the event meets the triggers of its actual DFARS 252.204-7012 clause and any customer or prime notice terms. The reporting decision belongs to its authorized organization, supported by IJK's technical facts and appropriate advice. A suspicious login does not automatically become a reportable cyber incident, but a team should not wait for certainty that every file was taken before beginning the assessment. The clause's rapid reporting definition uses seventy-two hours after discovery for the covered incidents. The clock and reporting process should be known before an event occurs. [2]

The response team preserves relevant system images and monitoring data under the clause when required, documents collection and custody, and avoids destroying evidence through an unplanned rebuild. It also needs to contain active harm and restore essential service. Those decisions can conflict, so the incident lead records why a device was isolated, imaged, or restored at each step. The clause's at-least-

ninety-day preservation period runs from submission of the report for the specified material; it is not a universal maximum or a general setting for all security logs. Other obligations may require longer retention. [2]

By the next day IJK may learn that an EGH migration application retained a permission that should have been removed. EGH supplies its change history and helps analyze the application only under an authorized relationship. Harbor Point updates its understanding of affected systems and takes the required follow-up actions. ABC does not conduct the investigation merely because an assessment is scheduled. If the event affects the accuracy of assessment evidence or a current status, Harbor Point evaluates those implications through the relevant process after stabilizing the response.

At the end of the first seventy-two hours, the team records its reporting decision, submissions and acknowledgments where required, additional facts needed, preservation status, customer notifications, and continuing investigation plan. It does not declare the case closed because an initial report was sent. Recovery, corrective changes, updated documentation, and management review can continue for weeks. A clear timeline allows leadership and later reviewers to understand what was known at each decision, rather than judging every action against facts discovered only afterward.

An incident timeline across all three parties

At 8:20 a.m. on a Tuesday, IJK's monitoring team sees unusual privileged access to Harbor Point's project workspace. The analyst opens an incident record, preserves the initial alert, checks the account and device involved, and follows the agreed escalation procedure. At 8:45 a.m., IJK alerts Harbor Point's authorized incident lead with known facts, uncertainty, and immediate containment options. Harbor Point determines whether the event affects covered information or operationally critical support under its actual contract and begins its reporting analysis. The clock for a clause-based rapid report cannot be reset by waiting for a perfect forensic conclusion. [2]

EGH may still have a migration-related application registration in the tenant. IJK checks whether the suspicious access used that path and whether EGH's stabilization agreement obliges it to help. EGH preserves its relevant change and access records and supplies technical facts through an approved channel. It should not issue a public conclusion or submit Harbor Point's government incident report without authority.

ABC, as a prospective assessor, is not the incident commander. If the event affects a pending assessment, Harbor Point addresses the implications through the appropriate assessment process after stabilizing the response.

The incident lead chooses containment steps while preserving evidence. It may disable an account, revoke sessions, isolate a device, capture logs and volatile information where feasible, and document the timing and reason for each action. The team identifies affected systems and images or monitoring data requiring preservation under the applicable clause. DFARS 252.204-7012 specifies a seventy-two-hour rapid report for reportable cyber incidents and preservation of relevant images and monitoring data for at least ninety days from submission. The clause's exact triggers and other directions must be read from the contract; this example does not label every unusual sign-in a reportable incident. [2]

After the initial report or decision that reporting is not required, Harbor Point continues investigation and records changes in understanding. IJK tracks containment, eradication, restoration, and tool health; EGH corrects any covered implementation defect; management documents effects on scope, controls, and ongoing representations. The next monthly packet can summarize the event and corrective action, but it should not replace incident-specific notices, required preservation, or later updates. A defensible report states known facts and uncertainty without manufacturing a complete story before the investigation is complete.

A cyber incident is not handled through the annual affirmation process. Where DFARS 252.204-7012 applies, its reporting and preservation requirements create a separate response obligation. The clause defines rapid reporting in terms of seventy-two hours after discovery and identifies the incidents to which its reporting provisions apply. It also requires a review for evidence of compromise. IJK should understand that trigger and process before an incident occurs. [2]

The seventy-two-hour period should not be treated as time available to postpone investigation or internal escalation. An operational alert must reach the people who can determine the facts, initiate containment, and evaluate reporting obligations promptly. The company should not wait for perfect certainty or a completed forensic report before addressing an applicable reporting deadline. Initial reporting, continued investigation, and later updates must be coordinated under the relevant instructions.

IJK should establish the reporting access, authorized submitters, and alternates in advance. The incident plan should identify the applicable DoD reporting channel, customer notification requirements, provider contacts, and the role of counsel where

appropriate. Providers should notify IJK early enough for IJK to satisfy its own obligations. A provider contract allowing notice only after several days of internal investigation may be incompatible with the customer's reporting needs.

Evidence preservation requires deliberate action. DFARS 252.204-7012 calls for preserving and protecting images of known affected systems and relevant monitoring or packet capture data for at least ninety days from submission of the incident report. This is a specific preservation obligation; it is not a universal ninety-day retention setting for all records. Other requirements or preservation needs may require longer retention. [2]

The response team should coordinate containment with preservation. Reimaging a computer immediately may restore service but destroy useful evidence. Leaving a compromised system connected merely to collect more data can also increase damage. The incident procedure should provide access to competent responders who can make and document these decisions, preserve integrity, and maintain records of collection, transfer, and access.

The clause also addresses submission of isolated malicious software and access to additional information for forensic analysis. Its instructions distinguish submission to the designated defense cybercrime organization from ordinary communication with a contracting officer. IJK should follow the prescribed process rather than attaching malicious files to routine email. Provider agreements should support the assistance and information access required by the applicable clause. [2]

After immediate response, IJK should produce an internal review explaining the event, affected systems, actions taken, remaining uncertainty, and corrective work. The review should identify improvements to detection, access, configuration, training, or provider performance. It should not claim that an incident automatically proves every control failed, nor should it dismiss a serious event because the organization previously passed an assessment. The purpose is to understand what happened and restore a defensible operating condition.

Separating assessment, affirmation, and incident reporting

The reporting calendar has at least three separate tracks. The first concerns the applicable CMMC assessment and status. IJK identifies which of its own systems or customer systems are covered, the required level and assessment path, the relevant CMMC UID, the status date, and any permitted conditional closeout. The second concerns the annual affirmation when required: the authorized official should review

the current implementation and evidence before making the statement in SPRS. The third concerns cyber incidents and contract-specific notification: an incident may require prompt escalation and a separate report even when the next annual affirmation is months away. [1, 2]

A contractor should distinguish a self-assessment from an independent certification assessment. ABC, if authorized and engaged as a C3PAO for a required Level 2 certification assessment, evaluates the defined organization and scope under the applicable process. EGH can supply configuration documentation, and IJK can explain its operations and present evidence, but neither can transform its own implementation checklist into ABC's independent assessment result. If IJK supports a customer, it should not represent that its own CMMC status automatically satisfies the customer's separate contractual requirement.

A rapid incident reporting clock under DFARS 252.204-7012 is measured from discovery for the incidents covered by that clause. The incident team needs an intake path, an authorized reporter, backup coverage, and a method for preserving affected images and relevant monitoring information. The ninety-day preservation period described in the clause runs from submission of the cyber incident report; it is not a general log-retention period and does not justify deleting material subject to another preservation obligation. Customer and provider agreements should require notice soon enough for the contractor to meet its own obligations. [2]

Before any external submission, the record should identify who reviewed facts, who authorized the statement, the source data, applicable contract or rule, submission channel, confirmation, and any correction made later. This chain of custody helps prevent an operational manager from making a contractual statement outside delegated authority and prevents an executive from affirming a condition that no one has recently checked. The frequency and content of an internal status packet can be chosen by IJK; government deadlines and exact submission requirements must be verified from the current clause and program instructions.

21.29 Evidence that remains useful after installation

An evidence request without an assessment panic

ABC requests evidence that Harbor Point controls privileged access. Harbor Point's evidence coordinator starts with a requirement-to-process map rather than searching for screenshots at random. The system security plan describes who authorizes privileged roles, how IJK assigns them, how EGH's temporary implementation access

was controlled, how activity is logged, and how roles are reviewed. The coordinator identifies the current administrator inventory, approval records, time-bound activation records, a sample review, and a sample removal. Each artifact has a date, system, owner, and explanation of what it proves. Unrelated records are not dumped into the assessment folder merely to create volume.

The coordinator checks the sample against current reality. One approval ticket names a role that was renamed during migration. The evidence package includes the change record connecting the old and new names, rather than editing the old ticket to look contemporary. Another record shows an EGH account remained active for two weeks after acceptance under a documented stabilization exception. Harbor Point presents that period honestly, along with the approval, restricted permissions, expiry, and subsequent revocation. An assessor can then evaluate the actual implementation. Concealing a discrepancy would make the evidence less trustworthy and could prevent the organization from discovering a real gap.

IJK supplies operational artifacts through an agreed secure channel. It ensures customer records are separated from other tenants and limits any personal or sensitive data not needed for the assessment. Harbor Point controls what is disclosed under the assessment process, while ABC handles received evidence according to its engagement and program obligations. EGH may provide the original build record or configuration rationale, but it should not rewrite operating evidence or speak as though it owned Harbor Point's daily process. The package contains both design evidence and records created while the control was running.

After the request closes, the evidence coordinator notes which records were difficult to find. Perhaps administrator role exports were retained but the reviewer approval was scattered across email. IJK adjusts its procedure so the next review produces a single traceable record linked to the authoritative export. Harbor Point updates the evidence index, not by duplicating every file indefinitely, but by naming the system of record and retrieval method. The aim is to improve ordinary operations and future assessment readiness at the same time.

Evidence retention follows several rules, not one universal number. Assessment artifacts, security logs, service tickets, incident images, contracts, and personnel records may have different required or approved periods. Harbor Point documents the governing basis and holds, IJK configures technical retention where assigned, and EGH supplies any necessary export or transition capability in its agreement. A storage setting that deletes material before a required investigation or contractual

review is a design problem; keeping every sensitive copy forever is also a governance problem.

Evidence should show how the organization operates, not merely how it intended to operate on the day a policy was signed. A written access procedure explains the process. An approved access request, a recorded group change, and a subsequent review demonstrate its use. The strongest evidence connects the requirement, implementation, responsible personnel, and actual operating records without forcing a reviewer to guess how they relate.

IJK should maintain an evidence index organized around its applicable requirements and assessment objectives. The index can identify the system security plan section, relevant procedure, configuration record, operating evidence, owner, and location. It should describe where the evidence lives rather than duplicate every artifact into uncontrolled folders. Where copies are required for assessment, IJK should record the version and protect the collection appropriately.

Evidence must be accurate about time. A current screenshot cannot prove that a review took place six months earlier. If a required record was not created, the organization should document the gap and correct the process rather than fabricate a historical record. Similarly, a template with an old date should not be presented as evidence that the procedure was approved at that time. Integrity matters as much as completeness.

EGH should provide installation evidence as part of the handover, but IJK becomes responsible for the continuing evidence it generates. ABC may request examination of selected records through the assessment process, subject to appropriate handling arrangements. The parties should agree how assessors will access sensitive evidence and how submitted material will be protected and retained. Support tickets and ordinary email should not become uncontrolled evidence repositories.

Retention should be managed by category. Assessment artifacts, administrative logs, incident material, contract records, employee training, and routine service tickets can have different governing periods and handling requirements. IJK should document the applicable retention rules and verify current CMMC assessment evidence retention requirements when preparing its retention schedule. Incident holds and other preservation obligations should override routine deletion where required.

21.30 Managing changes and provider transitions

A new application that changes the protected boundary

A project manager proposes a cloud design-review application because it allows engineers and external partners to comment directly on drawings. The apparent business benefit is speed, but the application may receive controlled files, store derivative comments, create preview images, send notification emails, and invite outside users. IJK's change record describes those data paths and the application's identity permissions, hosting, support access, export method, and retention. Harbor Point's contract and data owners decide whether the use is permitted. EGH, if retained for engineering, can evaluate integration and migration effort; it does not approve the information flow.

A pilot uses non-sensitive representative content first. The team tests who can invite external collaborators, whether links can be forwarded, how access is revoked, what logs are available, how content is backed up or exported, and whether a user can move a drawing into an uncontrolled workspace. The license proposal includes not just named users but storage, guest access, audit retention, and support costs. The system security plan and provider list are revised if the application is approved. IJK adds monitoring and offboarding steps, and Harbor Point trains project staff on the allowed workflow.

If the application does not meet the required conditions, the team should not bury the result under a broad internal exception. It can select another service, redesign the collaboration process, limit the application to non-controlled information, or defer the business request. The decision record states what was considered and why. Staff need a practical approved alternative so that a blocked application does not simply drive them to personal accounts or email attachments. Management should follow up to see whether the chosen workflow actually meets the project's need.

The same discipline applies when a provider changes. A replacement backup vendor or MSP alters administrator access, data location, monitoring, contracts, and evidence. The old service is not switched off until the new one has passed a defined acceptance test and necessary history has been preserved. IJK may be the outgoing provider for one Harbor Point service and the incoming provider for another customer; its process should support both roles. Harbor Point retains the authority to accept transition risk and the responsibility to understand the resulting scope.

A change register should link each material change to its approval, technical implementation, test, updated documentation, and post-change review. The register need not contain a long essay for every small user request. It should, however, make it possible to reconstruct why the protected system looks different from the environment ABC previously examined. This traceability helps leadership judge whether a change affects current status, contractual reporting, or the next assessment plan.

A transition after an unplanned resignation

IJK's senior tenant administrator resigns unexpectedly. Harbor Point's service does not have to change providers, but the loss of a person tests the same continuity principles. IJK reviews the administrator's accounts, roles, devices, vault access, API keys, active sessions, and approvals. It transfers assigned tickets and scheduled reviews to a qualified alternate, revokes access at the authorized time, and verifies that backup administration, incident escalation, renewals, and evidence retrieval still function. Harbor Point receives notice under the agreement if service coverage changes materially.

The replacement operator works from current documentation rather than the departed administrator's personal notes. A supervised test covers a new-user request, a privileged change, a log search, a restore, and vendor support contact. Any failure becomes a corrective action with an interim owner. IJK should not ask the former employee for an undocumented password as its primary recovery path. The business should own or control the necessary credentials and service relationships through approved processes before an employee leaves.

If the resignation coincides with EGH's stabilization period, the parties clarify which defects EGH still owns and who within IJK accepts handover. EGH should not silently become the long-term operator because the named IJK contact departed. Harbor Point may approve a temporary extension or other arrangement, but it needs a documented term, access scope, and cost. ABC's planned assessment logistics may need an updated interview roster, yet ABC remains independent and does not repair the staffing gap.

The lessons feed succession planning. IJK updates alternate coverage, training, shared documentation, and periodic practice. Harbor Point checks whether its customer-facing responsibility matrix still names real people and escalation contacts. A program that depends on one expert may appear efficient until that person becomes

unavailable. Continuous readiness includes the ability to perform and explain ordinary controls after personnel change, not only after a technology change.

A planned move from one MSP to another

Assume Harbor Point decides to replace IJK at the end of its service term. It names a transition lead and a replacement operator before disabling existing access. The first work product is a service inventory: tenant, domains, users, administrator roles, endpoints, RMM, EDR, backup, log sources, ticketing, documentation, vault, applications, contracts, subscriptions, open incidents, and corrective actions. For each item the parties identify ownership, current administrator, data location, export method, and cutover dependency. Harbor Point approves the plan because it bears the business risk of an interruption.

The replacement operator receives limited access to observe and verify before assuming control. IJK provides current diagrams and runbooks, demonstrates backup recovery and alert routing, and explains unresolved exceptions. Sensitive data and credentials move through approved channels under the service agreement. A transition test confirms that the new operator can handle an alert, onboard a device, retrieve logs, and contact vendors. Harbor Point accepts the new operator's capability before the old operator's essential service rights are removed. Both providers record what they exchanged and when.

At cutover, Harbor Point or the new operator changes delegated admin relationships, rotates or replaces relevant secrets, reassigns notification addresses, updates support contacts and billing, and checks automation dependencies. IJK removes its interactive and noninteractive access and provides evidence of disposition of retained customer information under the contract. Harbor Point reconciles the asset, license, and evidence registers. If the RMM platform belongs to IJK and cannot be transferred, the plan includes agent replacement and validation on every protected device rather than assuming the new provider can inherit the console.

The system security plan, responsibility matrix, evidence index, and incident contact list are updated to reflect the new provider and actual service. The change may require analysis of the assessment scope or current status under applicable program rules. Records from IJK's prior operating period remain relevant even when the service relationship ends. A well-managed transition preserves continuity of controls and evidence; a mere termination notice and new invoice do not.

Every meaningful change should be evaluated for its effect on the protected environment. Adding a new application may create a new data destination. Enabling an integration may grant broad permissions. Allowing a contractor to work remotely may introduce new devices or locations. IJK should consider these effects before approving the change, rather than discovering them when the system security plan no longer describes reality.

A practical change record explains the business purpose, affected systems, information flows, security impact, test plan, approver, implementation timing, and rollback approach. Small routine changes can use an approved standard process, while significant architectural changes require deeper review. The process should be proportionate, but it should still make material changes visible and traceable.

When EGH or another provider leaves, IJK should begin with an inventory of that provider's access and responsibilities. The transition should transfer current documentation, configurations, relevant evidence, subscription details, and open work. IJK should confirm that the replacement operator can perform essential tasks before terminating necessary service access. A rushed departure can leave both excessive old access and inadequate new coverage.

The technical cleanup must address more than interactive accounts. Application credentials, delegated relationships, API keys, certificates, remote access agents, shared vault permissions, and automation jobs can preserve provider access. IJK should identify which items must be revoked, rotated, transferred, or replaced, then verify that the intended result occurred. The transition record should also confirm the disposition of information retained by the departing provider under the contract.

Provider changes may require updates to the assessment scope documentation, service responsibility descriptions, system security plan, and evidence records. The organization should evaluate whether the change affects its current status or other obligations under the applicable rules. A service transition is complete only when operating responsibilities and evidence are again clear, not merely when the final invoice has been paid.

A reporting and incident rehearsal in the same month

The operating month should include a reporting rehearsal. IJK prepares a management summary that says which people and assets are inside the protected boundary, which controls operated, which checks failed, and which decisions are required. Harbor Point's manager asks where the figures came from. IJK produces the

identity export, asset register, endpoint coverage report, log-source inventory, backup test, and corrective-action record. If one figure cannot be explained, the team corrects its measurement method before the report becomes a recurring assertion.

Next, a simulated alert reports that an engineering laptop uploaded an unusual volume of files. The exercise begins with triage: which user and device were involved, what information may have been accessed, where did the transfer go, and what evidence needs preservation? IJK handles the technical investigation within its service contract and promptly informs Harbor Point under the agreed escalation rules. Harbor Point evaluates its own contractual and program reporting duties with the appropriate authorized decision makers. EGH participates only if its still-active stabilization responsibilities or specific technical knowledge are needed. ABC is not called to run the response merely because an assessment is planned.

The exercise deliberately tests timing. A finding on Friday evening cannot wait until the regular Monday report. The response roster should name primary and alternate contacts, after-hours route, authority to isolate a device, method of preserving relevant logs, and a way to obtain current contract clauses. The team records when it discovered the event, who was notified, what remained uncertain, and why decisions were made. A later management report can summarize the exercise, but it does not substitute for a required incident report when an actual reportable event occurs.

At the end of the month, Harbor Point and IJK review what the exercise changed. They might shorten a provider-notification target, add log retention capacity, restrict a remote-support path, or revise a handover procedure. The change record updates the design and the system security plan as necessary. The lesson is practical: ownership becomes credible when each party can act under pressure, document its decisions, and continue the service after the original installer has gone.

21.31 A worked example of the first operating month

A complete first-month record

In week one after handover, IJK inventories the expected eight controlled-workload users, two administrators, their devices, project repository, required log sources, and backup jobs. It checks current observations against the signed acceptance package. One laptop is missing an endpoint sensor because a rebuild after the pilot omitted a step. IJK isolates the cause, deploys the agent, checks all devices built with the same process, and changes the onboarding runbook. Harbor Point's manager receives the

exception and confirms whether the device performed controlled work during the gap. EGH assists because the defect falls within the defined stabilization period.

In week two, the service desk processes a new hire and a departure. The new hire receives only the approved project role after a manager's request; the departing engineer loses directory, application, and remote access, and returns the device. IJK samples the sign-in and entitlement records to validate the results. During a license review, it finds that an information-protection add-on was assigned to seven of eight engineers. It corrects the assignment, checks whether the missing user handled protected content without the intended policy, and reconciles the invoice and vendor entitlement. Harbor Point approves any recurring cost change.

In week three, a recovery exercise finds that restored project files inherit broad permissions in the test location. IJK restricts the copy, identifies the runbook step that caused the error, corrects the procedure, and repeats the test. The original failure and retest remain attached to the recovery record. A separate alert reveals that one log connector stopped after an application certificate change. IJK restores the connector and records the blind interval. The management report does not replace these two events with a blanket statement that backups and monitoring were successful.

In week four, Harbor Point reviews the month with IJK and EGH. IJK presents scope and asset changes, exceptions, root causes, current coverage, restore and alert tests, license status, and open work. EGH confirms which items are covered by stabilization and which are new requests. Harbor Point decides whether to close installation acceptance, fund additional capacity, and proceed toward the planned assessment preparation. ABC has not yet assessed the environment and is not asked to certify that the implementation is ready by virtue of its presence on a call.

The month creates a realistic evidence trail: approvals, execution tickets, inventory reconciliation, health reports, failed tests, corrective changes, retests, license records, and management decisions. It also exposes whether IJK can operate without EGH. If an essential task still requires an installer's personal knowledge, Harbor Point should keep the handoff issue open. The strongest first month is not the one with zero findings; it is the one in which the team can explain and resolve what it discovers.

Assume the approved project places eight controlled-workload users into the selected government environment and assigns two IJK leaders defined administrative responsibilities. EGH has completed pilot testing, migrated the approved information, and transferred the runbooks. ABC has not yet issued an assessment result. The

company enters an initial operating period to demonstrate that the environment can be maintained by the people who will actually run it.

During the first week, the technical leader discovers that one laptop is missing from the endpoint protection report. The asset register shows that the laptop belongs to an authorized user, so the absence is investigated immediately. The problem is traced to an incomplete onboarding step. IJK records the correction, confirms the device appears in the console, and checks the rest of the population for the same issue. The lesson becomes an addition to the device acceptance procedure.

In the second week, the administrative leader reviews the license register and finds a discrepancy between the purchased quantity and assigned entitlements for a security feature. EGH and the reseller confirm the licensing requirement for the actual design. IJK corrects the assignment or purchase as appropriate and retains the entitlement evidence. This is more useful than waiting for renewal to discover that a policy relied on an unlicensed capability.

In the third week, IJK performs a restore exercise. The backup completed successfully, but the recovered document's permissions do not match the intended recovery workflow. The team corrects the procedure and repeats the test. The final record describes both the initial problem and the successful retest. Removing the failed result would make the record less honest and would hide an important operational lesson.

In the fourth week, the two leaders conduct a management review. They examine open issues, confirm that EGH's remaining access matches the stabilization agreement, and decide whether the organization is ready for the next assessment preparation milestone. If a material gap remains, they assign corrective work and revise the schedule. The decision is based on evidence of operating capability, not the amount already spent or the desire to declare the project finished.

This example illustrates why maintenance begins before assessment. The operating period reveals issues that installation tests may miss and gives IJK practice using its own procedures. It also creates records showing how the company identifies and corrects problems. A functioning security program does not mean nothing ever goes wrong. It means problems are detected, handled by accountable people, and resolved in a way the organization can demonstrate.

The first ninety days after acceptance

In the first thirty days, IJK should prove it can operate the design without relying on EGH's memory. It uses the runbooks to onboard and offboard a test identity, investigates a representative alert, verifies device and log coverage, restores a representative file, and holds its first management review. EGH resolves defects within the stabilization agreement and documents each change. ABC's independent assessment role remains separate. A readiness advisor, if engaged, may challenge the evidence and scope, but that engagement should be reviewed for its effect on later assessment independence.

During days thirty-one through sixty, IJK should test repetition rather than one-time success. A second access review, another restore test, a patch cycle, and a sample incident exercise reveal whether the processes depend on one technician. The team checks that records can be found by a backup operator and that the license register matches the actual tenant, users, devices, and renewal notices. Management closes or funds outstanding gaps and updates the system security plan when operation differs from the original design.

During days sixty-one through ninety, the parties should finish the handoff. EGH's remaining privileges are removed or placed under a separate ongoing agreement with a new scope and review date. IJK confirms it can contact product support, obtain exports, recover from loss of a key employee, and change providers without losing control of its own data. It reviews the assessment schedule and reporting calendar against current contractual requirements. This ninety-day sequence is a teaching example; it does not replace an assessment deadline, contract milestone, or incident-response clock.

The chapter's central division is now visible. ABC's accountable period is the authorized assessment engagement and its permitted follow-up. EGH's accountable period is the implementation contract and any defined stabilization or separately purchased support. IJK's accountable period is the life of its own security program and each customer service commitment, including orderly transition at termination. When a cloud vendor or reseller changes, those periods do not erase IJK's continuing responsibility to understand, fund, monitor, and evidence the controls on which it relies.

21.32 Bringing the responsibilities together

At the end of each year, the parties should be able to show a continuous chain from the original scope decision to current operations. Harbor Point can identify the contracts and information that define its obligation. It can show why its selected government environment and connected providers were approved, which systems and users are in the boundary, and what changed. IJK can show the routine records created while operating those controls: approved access, device coverage, investigated alerts, patch decisions, restore exercises, service exceptions, license renewals, and management reports. EGH can show what it implemented, how it tested the build, what it handed over, and when its temporary access ended. ABC can independently examine the applicable scope and evidence under its authorized engagement without becoming the operator of the system.

That chain matters when an uncomfortable question arises. If a customer asks whether a backup copy contains controlled data, Harbor Point can follow the information map to the backup service and its contract. If a technician asks why an external sharing rule is strict, IJK can find the approved design decision instead of guessing. If a manager asks whether a current affirmation is supportable, the official can review present evidence and unresolved gaps instead of relying on the date of a prior assessment. A program is durable when its records make decisions understandable to people who did not participate in the original project. The organizations should keep those records current as technology, contracts, staff, and service providers change.

The decision test for any future dispute

When a dispute arises, the parties should begin with the actual service and decision. If an endpoint agent is missing, IJK identifies and corrects the operating issue under its service agreement; EGH handles a covered installation defect if the agreed stabilization terms apply; Harbor Point decides any business interruption and retains responsibility for its own contractual statements. ABC may later evaluate the relevant implementation in an independent assessment but does not repair the agent. Naming the precise action and contract resolves more than asking which company is responsible for CMMC in general.

If a GCC High subscription lapses, the purchasing and billing records show who received the notice and who had authority to renew. IJK's operational monitoring should detect an impending service or entitlement problem if that task is assigned to

it. Harbor Point approves the expense and may need to address a lapse's effect on the protected workflow. EGH's expired project agreement does not make it a perpetual billing administrator. A shared responsibility matrix should express these stages: detection, recommendation, approval, execution, validation, evidence, and escalation.

If Harbor Point changes MSPs, it should retain control of the tenant, domains, information, contracts, and authoritative records. IJK delivers agreed exports, current documentation, open issues, and transition assistance, then removes access and handles its retained copies under contract. The replacement operator validates alerts, backups, privileged paths, and support procedures before assuming responsibility. EGH participates only if retained for a new engineering task. ABC's prior assessment does not automatically validate the new provider architecture; Harbor Point evaluates the effect of the change on scope and status under current rules.

If an incident occurs during transition, both outgoing and incoming providers may possess relevant records and access. Harbor Point's incident lead coordinates the response and contractual analysis, assigns technical actions according to current agreements, and preserves evidence from each source. The parties should have anticipated this overlap in the transition plan. An argument about who owns the ticket queue should not consume a reporting deadline. The organization needs contacts, authority, and preservation instructions before cutover begins.

The chapter's operating model can be tested with five questions. Who owns the business and contractual decision? Who performs the technical action today? Who checks that it worked? Where is the evidence kept? Who takes over if the provider or employee leaves? The answers may differ by customer and system. Writing them down and testing them in ordinary work is what turns software, licenses, assessment services, and an MSP contract into a sustainable program.

The three-party approach works when each party understands both its contribution and its limits. ABC supplies an appropriately authorized and independent assessment function. EGH delivers and documents an implementation that IJK can operate. IJK maintains the environment, manages its business obligations, and supports required reporting with current evidence. Cloud vendors, resellers, and other providers remain important, but their involvement must be described through actual service boundaries and agreements.

The most useful question at every stage is who will perform the next action. When an alert arrives, someone must investigate it. When a subscription approaches renewal, someone must verify the required rights and approve the expense. When an employee

leaves, someone must remove access and address devices and data. When an affirmation is due, an authorized official must have a reliable basis for making it. Naming these responsibilities turns a collection of tools into an operating program.

For an MSP, this discipline has value beyond its own assessment. It improves the quality of customer services by making promises specific, handovers testable, and maintenance measurable. It also helps the MSP explain honestly what its services provide and what remains the customer's responsibility. That clarity protects the business relationship and makes it easier to respond when technology, personnel, or contract requirements change.

The next stage of the organization's work is to keep the approved design aligned with actual operations. The assessment may be a major milestone, but continuing performance depends on ordinary decisions made every day. A well-maintained program connects those decisions to documented responsibilities, suitable technology, sustainable funding, and evidence that remains accurate over time.

Chapter reference tables

The tables that follow summarize the responsibilities and license decisions explained in the chapter. They are working aids for planning and review. They do not replace the applicable contract, assessment rules, product terms, or the detailed operating procedures.

Responsibility and duration

Activity	Principal responsibility	Duration or trigger
Define scope and approve resources	IJK management with technical input	Before implementation and when material facts change
Independent certification assessment	Authorized ABC assessment organization	Assessment engagement and applicable program duties
Configure and test the approved design	EGH with IJK participation	Implementation statement of work
Correct covered implementation defects	EGH	Agreed correction or stabilization term
Approve and remove user access	IJK business owner and administrator	Employment and role changes plus scheduled review
Review alerts and maintain protection	IJK or contracted operating provider	Continuing operations under defined coverage
Maintain subscriptions and renewals	IJK purchasing and technical owners	License term and renewal cycle
Submit required affirmations	Authorized affirming official	Applicable annual and status requirements
Handle applicable incident reporting	Contractor with designated response team	Incident trigger and applicable deadlines

Activity	Principal responsibility	Duration or trigger
Transfer services and revoke old access	IJK and departing or incoming providers	Provider transition

Capability and licensing review

Capability	Possible implementation	Purchasing question
Collaboration	Appropriate government collaboration subscription	Which exact cloud, services, users, and term are covered?
Identity and access	Entra ID and approved authentication methods	Which policy and governance features require added rights?
Device management	Intune or a suitable alternative	Which users, devices, and platforms are entitled?
Endpoint protection	Defender for Endpoint or a suitable alternative	Are workstation and server rights both addressed?
Email protection	Licensed advanced mail protection where needed	Which protection functions are actually included?
Information protection	Available and licensed Purview capabilities or alternatives	Which locations and users are covered by each feature?
Security monitoring	Approved SIEM and operating service	What drives ingestion, retention, and staffing costs?
Vulnerability management	Approved scanner and remediation process	Is pricing based on assets, agents, or another metric?
Backup and recovery	Suitable protected backup service	Which workloads, capacity, retention, and restores are covered?

Capability	Possible implementation	Purchasing question
Remote administration	Approved RMM and secrets management	Which technicians, endpoints, and service boundaries are covered?

Reporting and review calendar

Record or action	Example internal cadence or external trigger	Accountable owner
Significant alerts and failed protective services	Daily example plus immediate escalation when needed	Technical operations lead
Open remediation and device health	Weekly example	Technical operations lead
Management exceptions and spending decisions	Monthly example	IJK leadership
Access and provider review	Quarterly example subject to actual requirements	Business owner and security lead
License review	Before purchase, material change, and renewal	Technical and purchasing owners
CMMC affirmation	Applicable annual requirement	Authorized affirming official
Conditional status closeout	Applicable permitted period and closeout rules	IJK management and assessment participants
DFARS cyber incident report	Applicable reporting trigger and seventy-two-hour requirement	Contractor's authorized response team
Incident media preservation	At least ninety days from report submission when clause applies	Incident evidence custodian

Sources and further reading

The following primary sources support the regulatory and product-specific distinctions in this chapter. Online product descriptions and contract clauses can change. Use the clause incorporated in the actual contract, applicable program rules, and the current licensing documentation for purchasing and implementation decisions. The operational examples and suggested internal review frequencies in the chapter are teaching guidance, not additional government requirements.

Primary sources [1]–[6] were reviewed on September 21, 2026; source [7] was reviewed on September 23, 2026. Verify current versions before a live purchase, assessment, affirmation, or incident decision.

[1] Acquisition.gov. DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements. Current status, affirmations, identifiers, conditional status, and contract reporting.

Read the official source

[2] Acquisition.gov. DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. Cloud obligations, reporting, preservation, and forensic assistance.

Read the official source

[3] Microsoft Learn. Office 365 GCC Service Description. Government service and support distinctions.

Read the official source

[4] Microsoft Learn. Office 365 GCC High and DoD Service Description. Eligibility and environment considerations.

Read the official source

[5] Microsoft Learn. Microsoft Intune for US Government Service Description. Device management service considerations.

Read the official source

[6] Microsoft Learn. Microsoft Defender for Endpoint for US Government Customers. Government capabilities and licensing considerations.

Read the official source

[7] Microsoft Learn. Cross-tenant OneDrive migration overview, government cloud limitations. https://learn.microsoft.com/en-us/microsoft-365/migration/cross-tenant-onedrive-migration

CMMC for MSPs:
From Readiness to Certification

Chapter 22
The CMMC-Ready MSP Technology Stack

Expanded Teaching Edition

Authored by Dr. Charles Edwards

Chapter Purpose

A CMMC-ready technology stack is not a shopping list. It is an interconnected operating environment in which identity, endpoints, networks, cloud services, administrative tools, monitoring, recovery, documentation, and evidence work together. This chapter explains what each major technology does, why it matters, how an MSP and defense contractor operate it, what can fail, how failures are detected and corrected, and what evidence normal operations should create.

The governing principle throughout this chapter is simple: function first, vendor second. Products change. The security functions, operational responsibilities, and need for demonstrable evidence remain.

22.1 Start With Architecture, Not Products

A defense contractor should begin by understanding its information, users, systems, administrative paths, external providers, and CUI boundary. Only after those relationships are understood should the organization select technology. Buying an EDR platform, SIEM, RMM, vulnerability scanner, backup product, or government-cloud subscription before understanding the architecture can create expensive tools that do not cover the right assets or produce the required operational outcome.

Harbor Point Engineering provides a useful practical example. Harbor Point uses NorthStar Managed Technology for defined MSP services and Beacon SOC for security monitoring. Before NorthStar proposes products, the parties identify where CUI enters Harbor Point, where it may be stored, which users require it, which endpoints may access it, how administrators reach those endpoints, which cloud services participate, where logs go, and who responds when something fails. The resulting architecture drives the tool selection rather than the other way around.

22.2 Responsibility Must Be Designed With the Technology

For every major component, the parties should answer five questions: who owns the business decision, who administers the technology, who monitors its health, who approves significant changes, and who retains or can produce the evidence. Shared responsibility is normal. Undefined responsibility is the problem.

Suppose NorthStar administers Harbor Point's firewall while Beacon receives firewall events. Harbor Point approves significant business-impacting changes. If the firewall stops forwarding logs, Beacon may detect the absence, NorthStar may repair the

configuration, and Harbor Point may need notification depending on the event. The workflow is effective only when those responsibilities and escalation paths are established before the failure.

22.3 Identity and Access Management

Identity is the front door of a modern environment. The identity system should establish who the user is, how the user authenticated, what roles and groups the identity possesses, what resources may be accessed, and what administrative actions are attributable to that identity. Ordinary users, administrators, service identities, application identities, guests, and emergency accounts should not be treated as interchangeable.

NorthStar technician Maria may support Harbor Point, Meridian, and Falcon. Her employment by NorthStar should not automatically grant unrestricted access to all three customers. Her individual identity should be strongly authenticated, mapped to appropriate customer roles, and logged. If she changes a Harbor Point firewall at 2:17 a.m., the environment should be able to establish that Maria performed the action under an authorized role rather than merely recording that a shared account called NorthStarAdmin was used.

22.4 MFA and Conditional Access

Multifactor authentication reduces the value of a stolen password by requiring additional proof. A mature implementation does not stop at ordinary users. The organization examines administrators, guests, service identities, emergency access, legacy authentication, exclusions, recovery procedures, and the lifecycle of exceptions.

Conditional Access adds context. Harbor Point may permit Daniel to reach an engineering resource from his managed, compliant laptop after successful MFA while blocking the same access from an unmanaged personal device. The important lesson is that identity, endpoint management, and information access work as one system. A policy shown as enabled in a portal is not enough; expected and prohibited scenarios should be tested and the resulting logs reviewed.

22.5 Privileged Access

Privileged access deserves stronger controls because compromise of a powerful administrative identity can allow an attacker to alter policies, disable defenses, create

accounts, change logs, or interfere with recovery. The objective of privileged-access management is not merely to hide passwords. It is to control who can exercise privilege, against which environment, for what purpose, under what conditions, and with what record.

During an emergency firewall change, Maria should authenticate with her individual identity, obtain the approved level of elevation, perform the authorized action, and leave an attributable record. The incident ticket explains why the change occurred; the firewall records what changed; the privileged-access platform records who exercised authority; and the SIEM and SOC retain the security context that caused the escalation.

22.6 Endpoint Management and Device Lifecycle

A managed endpoint should be understood throughout its lifecycle: acquisition, assignment, configuration, enrollment, protection, patching, monitoring, repair, reassignment, loss, and retirement. The organization should know who owns the device, who uses it, whether it can access CUI, whether storage encryption is enabled, whether management and EDR agents are healthy, whether required software is present, and when the device last communicated.

If Daniel's laptop appears in RMM but disappears from EDR, the fact that the computer still works is irrelevant to the security question. NorthStar should investigate whether the agent was removed, failed, lost registration, or was affected by a rebuild. The discrepancy becomes a ticket, receives an owner, is corrected, verified, and closed.

22.7 RMM: Powerful and Security-Critical

Remote Monitoring and Management gives an MSP extraordinary operational leverage. It can inventory systems, deploy software, execute scripts, patch endpoints, restart services, and provide remote access. The same power makes RMM a security-critical control plane. Strong authentication, role separation, customer segmentation, logging, script governance, API protection, and rapid offboarding are essential.

A technically correct script can still create a major incident if it is sent to the wrong customer group. Before a high-impact deployment, the technician should know the purpose, customer authorization, exact target population, test result, rollback method, verification method, and evidence that will remain. Automation should make the correct action repeatable, not make an uncontrolled action faster.

22.8 PSA/ITSM: The Security Value of the Ticket

A ticket is more than administrative overhead. It can connect the business reason for a change with the technical evidence of the change. A firewall log may prove that a rule changed, while the ticket explains who requested it, who approved it, why it was necessary, who implemented it, what testing occurred, and when it was closed.

Two technically identical firewall rules can therefore have very different security meaning. One may have authorization, scope, testing, validation, and review. The other may have been created from an informal request saying only 'make it work.' Good ticketing creates traceability and helps future administrators understand why a configuration exists.

22.9 EDR/XDR and Security Response

Endpoint Detection and Response provides visibility into endpoint behavior and supports investigation and response. Extended Detection and Response may correlate additional data sources depending on the platform. The operational questions are more important than the label: can suspicious behavior be detected, can the event be investigated, can the endpoint be isolated when authorized, can protection health be measured, and can evidence be retained?

When Daniel opens a malicious attachment, the EDR detects suspicious behavior and forwards telemetry into the monitoring workflow. Beacon investigates and escalates. NorthStar confirms the correct customer, reviews Harbor Point's incident procedure, obtains authorized access, and isolates the device if permitted. Identity logs, endpoint telemetry, SIEM records, SOC notes, RMM information, and the incident ticket collectively tell the story.

22.10 SIEM, SOC, and the Missing Log Source

A SIEM centralizes and analyzes security-relevant events. A SOC is the operational capability that monitors and investigates those events. Buying a SIEM does not create a SOC, and hiring a SOC does not guarantee that every important source is connected.

Harbor Point should maintain an expected log-source inventory. If ten critical servers are expected to report and only nine have reported within the normal interval, the absence itself becomes an event requiring investigation. Beacon may detect the missing source, NorthStar may repair it, and the ticket remains open until events are

actually visible again. Monitoring the health of the monitoring system is part of security monitoring.

22.11 Vulnerability Management

Vulnerability management is a lifecycle: discovery, validation, prioritization, remediation or controlled exception, verification, and closure. A scanner report with hundreds of findings is not the outcome. The outcome is informed reduction of exposure.

When the same serious vulnerability affects Harbor Point and Falcon, the response may differ. Harbor Point may be able to patch immediately. Falcon may operate a legacy manufacturing system whose vendor has not approved the update. Falcon's team may need network restrictions, additional monitoring, reduced privileges, a tested maintenance window, vendor engagement, and documented temporary handling while the permanent fix is developed. Context informs priority without becoming an excuse for inaction.

22.12 Patch and Configuration Management

Patch deployment is an action; risk reduction is the desired outcome. The MSP should distinguish applicable, downloaded, installed, reboot-pending, failed, and verified states. A 98 percent success rate can conceal the two systems that matter most.

If two of one hundred Harbor Point systems fail a critical update, NorthStar identifies the actual devices, determines why each failed, assesses their exposure, remediates or controls the exception, and verifies the result. Configuration management follows the same logic: approved baselines, controlled changes, drift detection, exceptions, validation, and documentation.

22.13 Backup, Recovery, and Administrative Separation

A green backup dashboard does not prove recoverability. The organization should know what is expected to be protected, whether all expected systems are enrolled, whether backup jobs succeed, whether recovery copies are protected, and whether restoration has been tested.

If Harbor Point deploys a new engineering server but nobody adds it to backup, the backup product may operate perfectly while the business remains unprotected.

Reconciliation between authoritative inventory and backup coverage detects this class of failure. Restore testing should go beyond proving that files can be extracted; where appropriate it should prove that the business capability can actually be recovered, including dependent databases, configurations, identities, and services.

Backup administration should also avoid unnecessary common failure paths. If the same compromised identity can destroy production and all recovery copies, resilience is weakened. Strong authentication, appropriate separation, protected retention, and immutable or otherwise deletion-resistant capabilities may be appropriate depending on the architecture.

22.14 Network Security and Segmentation

Modern network security is not simply a firewall between trusted inside systems and the Internet. Users, endpoints, cloud services, remote administrators, wireless networks, printers, servers, and external providers create many communication paths. The network should permit what the business requires while limiting unnecessary reach.

A multifunction printer may need DNS, time synchronization, print services, management, and approved scanning destinations. It does not automatically need unrestricted communication with engineering servers. Segmentation is meaningful only when communication between segments is actually controlled.

22.15 Firewall Change Lifecycle

A firewall rule should have a business purpose, defined source and destination, protocol and port, owner, approval, implementation record, validation, and eventually a reason to remain or be removed. Temporary troubleshooting rules should not quietly become permanent architecture.

If an administrator encounters a rule labeled TEMP-ALLOW-ANY two years later and nobody knows why it exists, poor documentation has become a security problem. Mature operations periodically review rules and remove obsolete exposure through controlled change.

22.16 Secure Remote Access and Technician Offboarding

Remote administration is essential to MSP operations and therefore must be protected as a high-value pathway. The MSP should know who can establish sessions, how

they authenticate, which customers they can reach, what privilege is available, what is logged, and how access is removed.

When technician Robert leaves NorthStar, disabling his email account is not enough. The offboarding process should address RMM, documentation, credential vaults, firewall portals, backup systems, vulnerability platforms, security portals, customer VPNs, SaaS applications, vendor portals, API tokens, and any approved emergency credentials. Offboarding means removing the person's ability to exercise organizational authority.

22.17 Secure CUI Exchange

Authorization to receive information and authorization to use a particular transfer method are different questions. If Daniel is told by an authorized partner to upload CUI to a personal file-sharing account, the recipient's authorization does not automatically make the transfer method appropriate.

The contractor should establish approved methods for protected information exchange and teach employees how to recognize them. The selected service must be evaluated in the context of the information, contractual obligations, identity controls, encryption, external sharing, retention, logging, administration, and provider responsibilities.

22.18 Email, Collaboration, Guests, and External Sharing

Email and collaboration systems combine identity, messaging, files, groups, guests, and external sharing. Governance should address who can create collaboration spaces, invite guests, create anonymous links, change sharing settings, and retain access after a project ends.

A guest engineer added for a six-month project should not remain authorized three years later merely because nobody removed the account. Access that was appropriate yesterday is not automatically appropriate tomorrow. Event-driven removal and periodic access review work together to control accumulation.

22.19 Software, Browser Extensions, SaaS, and AI

Software governance should ask what an application does, what information it can process, what privileges it requires, where it sends data, how it is updated, who owns

it, and whether an approved alternative already exists. 'Not malware' does not mean 'appropriate for a CUI environment.'

The same reasoning applies to browser extensions, SaaS, and AI. If Priya submits CUI to an unapproved public AI service, the problem is not that AI is inherently bad; the problem is that protected information has been sent to a system that was not approved for that information. Governance must follow the information flow, including AI capabilities embedded inside browsers, productivity suites, development tools, and SaaS platforms.

22.20 Documentation and Knowledge Management

MSP documentation may contain network diagrams, IP information, procedures, escalation contacts, customer-specific configurations, recovery information, and links to privileged systems. It is part of the security architecture and should receive appropriate access control, authentication, customer separation, lifecycle management, and auditability.

Personal technician notes create both continuity and security problems. If Maria keeps a critical workaround only in a text file on her desktop, NorthStar has knowledge that the organization cannot reliably govern or reuse. Controlled documentation converts individual knowledge into organizational capability.

22.21 Automation and Orchestration

Automation improves consistency and scale, but a mistake can also be repeated across thousands of systems in seconds. Scripts and automated workflows should therefore be designed, tested, scoped, approved according to impact, logged, verified, and supported by rollback planning where appropriate.

A one-line PowerShell command may have more operational impact than a two-hour manual procedure. Risk should be based on what the automation can do, not on how many lines of code it contains.

22.22 APIs and Integrations

Modern tools depend on application registrations, API tokens, OAuth grants, service accounts, connectors, and webhooks. These machine-to-machine relationships are identities and trust relationships in their own right. They require ownership, least privilege, credential protection, monitoring, and retirement.

If Harbor Point tested a reporting application two years ago and stopped using it, the API authorization should not remain forever. The organization should periodically ask of every important integration: what is this, why does it exist, who owns it, what can it access, is it still required, and how will we know if it fails?

22.23 Asset Reconciliation

Reconciliation is one of the strongest operational controls in the stack. Harbor Point may have 125 workstations in authoritative inventory, 125 in RMM, 124 in EDR, 123 in vulnerability management, and 125 in device management. The important information is not that the numbers are close. The important information is which exact devices create the difference and why.

Exceptions should become owned work. A rebuilt laptop that was restored to RMM but never re-enrolled in EDR can remain invisible for months if nobody compares populations. Reconciliation discovers silent failures before an incident does.

22.24 Evidence Architecture

Evidence should arise from normal operations rather than being manufactured before an assessment. Identity systems can show account and authentication activity; device platforms can show enrollment and compliance; EDR can show coverage and detections; vulnerability systems can show findings and verification; patch platforms can show deployment and exceptions; backup systems can show jobs and restore tests; firewalls and SIEM can show events; ticketing can show authorization and work history.

Evidence must still be purposeful. The contractor and MSP should know what claim an artifact supports, where it originates, who owns it, how long it is retained, and how it will be retrieved. Millions of screenshots without a mapping to operational claims are not a mature evidence program.

22.25 Who Owns and Retains the Evidence?

Evidence ownership should be established before assessment preparation. Harbor Point may own organizational approvals and policies. NorthStar may generate technical operational records. Beacon may retain SOC investigation records. Microsoft and other providers may expose cloud logs or service records. The responsibility model should identify who creates, retains, protects, and can produce each important evidence type.

Retention should be intentional and based on applicable contractual, legal, regulatory, assessment, security, and business requirements. A practical concern is licensing: a platform may provide only a limited searchable history under the purchased plan. If the evidence strategy assumes longer availability, the organization must address that mismatch before records expire.

22.26 Selecting Technology Without Buying 'CMMC in a Box'

No single EDR, firewall, SIEM, RMM, government-cloud tenant, vulnerability scanner, backup platform, or compliance dashboard makes an organization CMMC compliant. Technology can implement and evidence important functions, but it does not decide every business authorization, contractual obligation, scope question, or responsibility.

An MSP evaluating a new platform should examine customer separation, administrative security, authentication, logging, evidence retrieval, API behavior, government-cloud compatibility, data handling, integration, lifecycle support, failure detection, and exit strategy in addition to price and features. Product evaluation becomes an architecture and operating-model decision.

22.27 Technology Lifecycle and Replacement

Technology enters the environment, is configured, integrated, updated, licensed, monitored, changed, and eventually retired. Agents become outdated, APIs are deprecated, certificates expire, vendors change services, and administrators leave. Every stage can affect security and evidence.

When NorthStar replaces its RMM, both old and new platforms may temporarily have privileged access. The migration should account for device coverage, technician roles, scripts, integrations, MFA, API connections, stored secrets, evidence preservation, old-agent removal, and reconciliation of the final population.

22.28 When the Security Tool Becomes the Security Problem

Security products are attractive targets because they often possess broad authority. RMM can execute commands, identity platforms can alter access, backup systems can reach important data, EDR consoles can affect endpoints, and documentation platforms can reveal architecture. Security tools need strong authentication, patching, monitoring, recovery planning, controlled administration, and lifecycle management just like the systems they protect.

The organization should also plan for tool failure. If Beacon escalates an incident while NorthStar's RMM is unavailable, the response plan should identify an approved alternate method for critical actions where necessary. Resilience includes the tools used to provide resilience.

22.29 Commercial Microsoft 365, GCC, and GCC High

Cloud selection begins with requirements and information, not with a slogan that CMMC automatically requires a particular Microsoft environment. Microsoft currently distinguishes its commercial and U.S. Government offerings and states that GCC High is designed for U.S. Government requirements including contractors holding or processing DoD CUI or subject to ITAR, with eligibility validation before establishment. The contractor should evaluate contractual and data-handling requirements with appropriate qualified support rather than treating the cloud name as a substitute for analysis.

GCC and GCC High are not simply license tiers. They can involve different service architecture, endpoints, feature availability, integrations, and operational procedures. The correct decision therefore considers contracts, CUI and other regulated information, eligibility, required services, collaboration partners, third-party applications, security tooling, APIs, administration, migration complexity, and lifecycle cost.

22.30 Government-Cloud Integration Reality

Microsoft documents that GCC continues to use the worldwide Microsoft Graph endpoint, while GCC High uses the U.S. Government Graph endpoint graph.microsoft.us. Applications must authenticate against the correct national-cloud environment, and Microsoft notes that service/API support can differ across national clouds.

This explains a common practical failure. A reporting application that works perfectly in commercial Microsoft 365 may fail in GCC High even when the credentials are correct because the product does not support the government endpoint or required API. Before purchase or migration, the MSP should verify the exact cloud, service, endpoint, permission model, data location, and feature set supported by each integration.

22.31 Intune and Device Migration to GCC High

Microsoft's current Intune Government documentation states that GCC High and DoD use the government Intune service instance, while GCC uses the commercial Intune service. Microsoft also states that devices moving between commercial Intune and the government cloud must unenroll from the current tenant and re-enroll in the new tenant; there is no built-in migration path between those service instances.

That turns a simple statement such as 'move our 80 laptops Friday night' into an operational project. The team must know which devices are available, how users will authenticate during transition, what happens if enrollment fails, how endpoint protection remains active, which policies and applications must be recreated or adapted, and how the final population will be reconciled.

22.32 Government-Cloud Network Endpoints

Microsoft publishes cloud-specific Microsoft 365 endpoints, including separate GCC High destinations. Restrictive firewalls, proxies, TLS inspection, and filtering systems can therefore affect government-cloud authentication and application behavior if required endpoints are not handled correctly.

If Word launches but a user cannot authenticate to a government service, reinstalling Office may not solve anything. The root cause may be a blocked government-cloud endpoint. Troubleshooting must follow the stack from application to identity to network rather than assuming the visible symptom identifies the failing component.

22.33 Three-Phase Implementation and Operational Handoff

Phase 1 is requirements, readiness, scoping, and architecture. The organization determines what must be protected, what contractual and security requirements apply, what systems and integrations exist, and what future architecture is needed. Phase 2 is technical implementation: tenant, domains, identity, MFA, access policies, email, collaboration, device management, endpoint protection, monitoring, integrations, migration, and validation. Phase 3 is knowledge transfer and operational acceptance.

Implementation should not close because the migration provider says the work is complete. Ongoing administrators should demonstrate that they can create a test user, assign the correct access, establish MFA, enroll a device, verify endpoint protection, locate logs, retrieve evidence, disable the account, and troubleshoot a controlled

failure. The question is not merely whether the environment was built; it is whether the organization can safely operate what was built.

22.34 What Must Be Handed Over?

The operational team needs the tenant architecture, administrative identities and roles, domains and DNS, licensing, identity design, MFA and access policies, Exchange configuration, Teams, SharePoint, OneDrive, device management, endpoint security, logging, integrations, APIs, network dependencies, migration history, diagrams, exceptions, recovery information, escalation paths, and unresolved issues relevant to its responsibilities.

Secrets should be transferred through approved secure mechanisms rather than embedded casually in documentation. Most importantly, every continuing function should have an owner: identity, privileged roles, failed enrollments, endpoint health, collaboration governance, integrations, licensing, DNS, security alerts, evidence, and service-change review.

22.35 Ongoing Microsoft 365 Government Maintenance

Implementation is not maintenance. After go-live, users join and leave, phones are replaced, devices fail, licenses change, guests accumulate, Teams and SharePoint sites are created, integrations break, vulnerabilities appear, Microsoft changes services, and administrators change roles. Ongoing maintenance is the permanent state of the environment.

The contractor determines business authorization; the internal administrator or MSP implements approved changes. If Daniel asks NorthStar for access to a sensitive SharePoint site, NorthStar's technical ability to grant access does not authorize the business decision. Harbor Point must provide the appropriate authorization, NorthStar implements it, the technology enforces it, and logs and tickets preserve evidence.

22.36 Change Governance

Ordinary administration and significant architectural change should not be treated identically. Routine user provisioning may proceed under an approved procedure. A change that alters CUI flow, security architecture, external-provider responsibilities, scope, logging, privileged access, or a major control implementation should trigger a more deliberate review.

A useful loop is request, security and CMMC impact review where applicable, authorization, implementation, technical validation, documentation update, evidence retention, and post-change monitoring. This prevents the technical environment from drifting away from the SSP, diagrams, responsibility matrix, and other governing documentation.

22.37 Random Tuesday Test

The strongest readiness test is an ordinary day with no warning and no assessment cleanup. Can Harbor Point identify the systems expected to be protected? Can NorthStar identify missing EDR agents, failed patches, stale vulnerability coverage, and backup exceptions? Can Beacon identify missing log sources? Can the parties show privileged administrators, recent significant changes, external guests, and the evidence supporting those activities?

If the answers require weeks of cleanup, the organization has learned that its documentation and evidence are retrospective. If the answers are available through normal operations, the organization is moving toward continuous readiness.

22.38 Complete Practical Incident Walkthrough

Daniel receives a convincing email and opens a malicious attachment. EDR detects suspicious behavior. Telemetry reaches Beacon. Beacon investigates and escalates. NorthStar receives the incident, verifies Harbor Point as the customer, reviews the approved response procedure, and assigns Maria. Maria uses her individual strongly authenticated identity and obtains only the privilege required for the response.

The endpoint is isolated if authorized and appropriate. Identity activity is reviewed. Related indicators are searched in the SIEM and EDR. NorthStar and Beacon determine whether other systems show similar activity. Harbor Point evaluates whether protected information may have been affected and follows its incident-handling and reporting procedures. Remediation is performed, the endpoint is validated before return to service, and the team examines why the event succeeded.

The resulting evidence includes endpoint telemetry, SIEM events, SOC investigation notes, identity records, administrative logs, ticket history, incident records, configuration changes, and validation results. The important lesson is that no single product 'handled CMMC.' A coordinated operating system of technology, people, responsibilities, and evidence handled the event.

22.39 Complete Practical Onboarding Walkthrough

Priya joins Harbor Point. Her manager authorizes the role and required project access. The onboarding request enters the ticketing workflow. Her individual identity is created in the correct tenant. Appropriate licensing is assigned. MFA is established. Group membership is based on authorized need rather than convenience.

A company-managed laptop is assigned and recorded in inventory. The device is enrolled in management, encryption is verified, endpoint security and RMM are confirmed healthy, vulnerability coverage begins, approved applications are installed, and required policies are applied. Priya tests access to approved resources. The technician validates the result and closes the ticket with evidence.

A week later, reconciliation confirms that Priya's device appears in inventory, RMM, EDR, vulnerability management, and device management as expected. Nothing dramatic happened, yet the organization created security and evidence through ordinary operations.

22.40 Complete Practical Offboarding Walkthrough

When Priya later leaves Harbor Point, the termination event initiates the reverse lifecycle. Her identity is disabled according to procedure, sessions and access are addressed, group memberships and privileged roles are removed, assigned equipment is recovered or controlled, remote access is removed, third-party and guest access is reviewed, and ownership of business information is transferred as needed.

The process is not complete merely because email no longer works. The organization verifies that Priya can no longer exercise authority through the relevant systems. The ticket, identity records, asset records, and supporting administrative logs provide evidence of the completed lifecycle.

22.41 Final Operating Model

The defense contractor owns its business requirements, contractual obligations, information, authorization decisions, and overall security responsibility. The CMMC readiness specialist helps interpret requirements, scope, gaps, documentation, and preparation. The implementation provider builds the approved technical environment. The internal IT team and/or MSP operates assigned functions. The MSSP or SOC monitors assigned security activity. Cloud and other external providers perform their

documented service responsibilities. An independent assessor assesses rather than operates the program.

The useful question is therefore never simply 'Who is our CMMC company?' The useful questions are who performs each function, who owns the decision, who administers the technology, who monitors health, who responds to failure, who approves significant changes, who retains evidence, and who verifies that the process still works.

22.42 Closing Perspective

A CMMC-ready technology stack is not something an organization purchases. It is something the organization designs, implements, operates, validates, maintains, and improves. Every important technology should have a defined purpose and owner. Every expected asset should be accounted for. Every critical security service should be monitored for health. Every failure should have an escalation path. Every exception should have an owner and review point. Every significant change should be evaluated. Every ongoing administrator should understand the environment. Normal operations should continuously create usable evidence.

The final chain is therefore: business and contractual requirements -> information and CUI -> architecture -> identity -> endpoint -> network -> cloud -> applications -> protection -> monitoring -> administration -> response -> recovery -> documentation -> evidence -> validation -> continuous operation. That is the difference between owning security technology and operating a security program. It also creates the bridge to Chapter 23, where the focus moves from building the stack to maintaining certification and continuous readiness.

Chapter 22 Operational Questions - Answered Reference

The following reference is intentionally concise. It does not replace the detailed teaching above; it gives the reader a final operational map after the concepts have been explained.

Operational Question	Operational Answer
How do we know what should be protected?	Maintain an authoritative inventory, define required protection by asset type, reconcile it against RMM/EDR/vulnerability/device-management/backup populations, investigate every unexplained difference.

How do we know endpoint protection is healthy?	Measure agent presence, recent check-in, policy assignment, protection status, version/health, and unresolved exceptions; create tickets for missing or stale agents and verify restoration.
How do we know MFA covers the right identities?	Define the required identity population, review policy scope and exclusions, test ordinary and privileged scenarios, control exceptions, and periodically revalidate them.
Who should have administrator access?	Only individuals whose current responsibilities require the privilege; use individual identities, least privilege, strong authentication, controlled elevation, logging, event-driven removal, and periodic review.
How do we know SIEM coverage is complete?	Maintain an expected log-source inventory, monitor source freshness, alert on missing/stale sources, assign repair ownership, and verify that events resume before closure.
How do we prioritize vulnerabilities?	Combine technical severity with exploitability, exposure, asset importance, information handled, available mitigations, active exploitation information, and operational impact.
How do we know patching worked?	Verify the desired outcome through installed version/configuration and, where appropriate, rescanning or other technical validation rather than relying only on deployment status.
How do we know backups will recover the business?	Reconcile coverage, monitor job health, protect recovery administration, and perform documented restore tests that validate the required business service and dependencies.
How do we approve software and AI?	Evaluate purpose, owner, information processed, privileges, external data flows, update model, vendor/service risk, contractual suitability, and lifecycle; authorize use for defined information and contexts.
How do we secure RMM?	Strong MFA, individual identities, least privilege, customer segmentation, script/change governance, API protection, logging, platform monitoring, rapid offboarding, and alternate incident methods where needed.
How do we keep documentation accurate?	Update it after meaningful changes and periodically validate diagrams, inventories, SSP descriptions, responsibility assignments, and procedures against

	actual system behavior.
What evidence do we keep?	Keep evidence that supports defined security and operational claims; map sources and owners, set intentional retention, protect records, and test retrieval before assessment.
Who owns integrations?	Assign an operational owner for every material connector/API/app registration, document purpose and permissions, monitor health, rotate/protect credentials, and remove obsolete trust.
How do we handle vendor change?	Assess material service, feature, API, licensing, endpoint, and security changes for impact on architecture, CUI flow, controls, integrations, evidence, and documentation; then validate and update.
Who is responsible when providers overlap?	Decompose the service into performer, approver, monitor, escalator, evidence owner, and verifier. Contractor accountability remains with the contractor even when operational functions are outsourced.

Authoritative Technical Notes for Publication

Microsoft 365 Government details are time-sensitive and should be rechecked before future editions. As verified for this edition, Microsoft documents separate U.S. Government offerings and eligibility; GCC High is intended for scenarios including DoD CUI and ITAR requirements. Microsoft Graph uses the worldwide endpoint for GCC and the U.S. Government endpoint graph.microsoft.us for GCC High. Microsoft Intune documentation states that GCC High and DoD use the government service instance, while GCC uses the commercial Intune service, and that moving devices between commercial Intune and the government cloud requires unenrollment and re-enrollment because there is no built-in migration path. Microsoft also publishes cloud-specific Microsoft 365 network endpoints for GCC High.

Official references: Microsoft Learn, Office 365 US Government Service Descriptions; Office 365 GCC High and DoD; Microsoft Graph National Cloud Deployments; Microsoft Intune for US Government GCC High and DoD; Microsoft 365 U.S. Government GCC High Endpoints. These references should be checked again during final book production because cloud features and service descriptions change.

Chapter 22 Expanded Teaching Laboratory: From Product Names to Operational Mastery

The preceding sections establish the architecture and the major components of a CMMC-ready MSP technology stack. This expanded teaching portion deliberately slows the discussion down. The objective is to answer the questions a new defense contractor, a new MSP technician, an experienced administrator moving into the Defense Industrial Base, or a manager responsible for a CMMC program is likely to ask after hearing the name of a technology. Knowing that an organization uses an RMM platform, an EDR platform, a SIEM, Microsoft 365 Government, a vulnerability scanner, or a backup service is not enough. The reader must understand what the system is doing, how it connects to the other systems, how it is operated, how it fails, how a technician discovers the failure, and how the organization demonstrates that the security function remains effective.

22.43 Building the Authoritative Asset Inventory

An authoritative asset inventory is the operating population against which security coverage is measured. It should not be confused with a list exported from whichever management product is most convenient. If NorthStar exports the RMM list and declares that list to be Harbor Point's inventory, a computer that never received the RMM agent can disappear from both the management platform and the supposed inventory. The organization would then be comparing the tool with itself and could incorrectly conclude that coverage is complete.

Harbor Point therefore needs an inventory process that begins when equipment or a virtual system enters organizational control. The record should contain enough information to distinguish one asset from another and to support security decisions. Depending on the environment, useful attributes include asset identifier, hostname, serial number, device type, assigned user, owner, physical or logical location, operating system, business purpose, CUI relevance, management status, encryption status, expected EDR coverage, expected vulnerability-scanning coverage, expected backup coverage, and lifecycle state. The exact fields can vary, but the record must be capable of answering what the asset is and what protections are expected.

Consider a new engineering laptop. Purchasing receives the hardware, IT records it, the device is assigned an asset identifier, and the provisioning workflow establishes the expected security services. The laptop should eventually appear in the authoritative inventory, identity/device-management platform, RMM, EDR, vulnerability-management platform, and other applicable systems. Each appearance answers a different question. Inventory says the laptop exists. Device management

says it is enrolled and receiving policy. RMM says NorthStar can manage it. EDR says endpoint protection is present and reporting. Vulnerability management says the system is being evaluated for known weaknesses.

The operational control is reconciliation. NorthStar periodically compares these populations by unique identifiers rather than totals alone. If the inventory contains 125 workstations, RMM 125, EDR 124, and vulnerability management 123, the technician identifies the exact missing records. An exception is opened for each unexplained difference. The investigation may reveal a failed agent, a duplicate record, a retired device that was never removed, a rebuilt system registered under a new identifier, or a newly deployed machine that skipped part of provisioning. Each explanation produces a different correction.

Evidence from this process is more persuasive than a screenshot showing a product dashboard. The evidence can include the inventory extract, reconciliation report, exception ticket, technician investigation, corrective action, and final verification. The organization can then explain not only that it intends to protect its assets but also how it detects when expected protection disappears.

22.44 A Day in the Life of an MSP Technician Supporting a CMMC Customer

Maria begins her morning at NorthStar by authenticating to NorthStar's administrative environment with her individual account and required MFA. Before touching a customer system, she reviews the ticket queue, security escalations, failed automation, and monitoring exceptions. The customer context matters immediately because Harbor Point, Meridian, and Falcon do not have identical architectures, contracts, cloud environments, or authorization procedures.

Her first ticket concerns a Harbor Point engineering workstation that stopped reporting to EDR overnight. Maria does not immediately remote into the machine and reinstall software. She first verifies the asset, assigned user, current state, last EDR communication, RMM status, recent changes, and whether Beacon has observed related alerts. The RMM agent is healthy, so she has a management path. The EDR console shows the endpoint last checked in shortly after a Windows update and reboot.

Maria opens an approved remote session through NorthStar's RMM. The session is attributable to her identity. She checks whether the EDR service is installed and running, examines relevant local logs, verifies network connectivity to required service endpoints, and confirms that the endpoint has not been deliberately isolated or

placed into a special response state. She discovers that the EDR service failed to start after the update. She follows the documented recovery procedure, restores the service, and waits for the device to reappear in the EDR console.

The ticket is not closed when the service starts locally. Maria verifies that the management console receives a fresh check-in, confirms the correct policy assignment, and determines whether there was a period of reduced visibility requiring additional review. Beacon confirms that telemetry has resumed. Maria records the cause, action, verification, and any follow-up work. A routine support ticket has now produced evidence of detection, ownership, troubleshooting, correction, and validation.

Later the same morning Maria receives a similar ticket for Falcon. She does not assume the same fix. Falcon uses a different endpoint platform and has a production system with change restrictions. Multi-customer MSP operations require standardized thinking without pretending that every customer's technology and authorization model are identical.

22.45 RMM Architecture, Deployment, and Maintenance in Detail

An RMM platform normally consists of a central management service, endpoint agents or other management mechanisms, technician identities and roles, automation capabilities, remote-control functions, monitoring policies, alerting, software-deployment functions, and integrations with ticketing or documentation systems. In an MSP environment, the platform may contain many customers under one administrative service. That makes tenant or customer separation a fundamental design concern.

Deployment begins with deciding which assets are supposed to be managed and how the agent will reach them. The MSP may use provisioning packages, device-management policies, scripts, imaging workflows, or manual installation for exceptional systems. The important control is not the installation technique. It is proving that every expected system has entered management and that unauthorized systems have not been enrolled.

Once deployed, the agent itself requires lifecycle management. The MSP should know whether agents automatically update, how failed upgrades are detected, what network destinations are required, how certificates or tokens are handled, how proxy settings affect communication, and what happens when an endpoint has not checked in within the expected interval. A stale RMM record can represent a powered-off laptop, a retired system, a broken agent, a network problem, or an asset that has escaped management. The technician must determine which.

RMM automation deserves a separate control process because it magnifies both skill and error. A script should have a defined purpose, version, owner, testing history, target criteria, expected result, logging behavior, and rollback or recovery approach appropriate to its impact. A script that removes an obsolete application from ten test computers may be low risk. A script capable of changing firewall settings on every customer server requires substantially stronger governance.

NorthStar also needs to monitor the RMM platform itself. Failed logins, unusual technician activity, new administrative accounts, role changes, API tokens, integration changes, mass script execution, and security advisories concerning the RMM vendor deserve attention. A tool with broad administrative authority should not be treated as an invisible utility.

22.46 PSA and ITSM: Turning Work Into an Auditable Process

A Professional Services Automation or IT Service Management platform becomes the connective tissue between business authorization and technical activity. The ticket should answer why work exists before a technician performs it. That distinction matters in a regulated environment because a technically valid action may still be unauthorized.

Suppose Daniel asks Maria to open a firewall port because a new engineering application cannot communicate with a server. Maria should not interpret Daniel's technical request as automatic authorization to change the firewall. The workflow identifies the business owner, confirms the approved requirement, records the requested source and destination, protocol and port, expected duration, and security impact, and routes the request through the appropriate approval path.

After approval, Maria performs the change through her individual administrative identity. She tests the application and also verifies that the rule is no broader than intended. If the requested port solves the problem, she records the validation. If the rule is temporary, the ticket includes an expiration or review point. The firewall's configuration record proves that a technical change occurred; the ticket explains why it was allowed.

Ticket quality therefore matters. A ticket that says 'fixed' is weak operational history. A useful record explains the condition, action, result, exception, and verification in enough detail that another authorized technician can understand what happened without relying on the original technician's memory.

22.47 EDR/XDR From Installation to Incident Response

Endpoint security begins with deployment, but the more important question is continuing effectiveness. An EDR agent must be installed, communicating, receiving the intended policy, able to collect the required telemetry, and capable of performing response actions that the organization expects. The management console should therefore be treated as a population to reconcile rather than a decorative dashboard.

When EDR detects suspicious behavior, the event enters an operational workflow. A detection may be generated locally or in the vendor's cloud analytics. The alert may then be forwarded to a SIEM or directly monitored by Beacon. An analyst examines process activity, user identity, network connections, file behavior, related indicators, and the history of the endpoint. The objective is to distinguish malicious activity from benign behavior while acting quickly enough to reduce risk.

Suppose Daniel opens a malicious attachment. The document launches a child process that behaves abnormally. EDR detects the behavior and creates an alert. Beacon sees the alert, checks whether the same indicator appears elsewhere, reviews Daniel's identity activity, and escalates according to Harbor Point's incident procedure. NorthStar receives the escalation and confirms the affected asset and user.

If Harbor Point's procedure authorizes immediate isolation under defined conditions, Maria isolates the endpoint. If approval is required, she obtains it through the incident workflow. The team then investigates whether credentials may have been exposed, whether the user accessed CUI during the affected period, whether other endpoints show the same activity, and whether the email reached other recipients. The response can involve identity, email, endpoint, SIEM, firewall, and ticketing systems.

After remediation, the endpoint is not returned to service merely because malware was deleted. The team validates security-agent health, patches and configuration, identity state, persistence indicators, network behavior, and any other relevant conditions. The incident record captures the chronology and evidence. This is how a technology stack behaves as a system rather than a collection of consoles.

22.48 SIEM Engineering and SOC Operations

A SIEM must first receive data before it can analyze data. This sounds obvious, but many monitoring failures begin with an assumption that a configured connector will continue working forever. Log-source onboarding should therefore document the source, expected event types, collection method, parser or connector, owner, normal reporting interval, retention, and monitoring responsibility.

Beacon may receive identity events, endpoint alerts, firewall events, server security logs, cloud audit events, and other sources. Those events are normalized or otherwise made searchable and can be evaluated by detection logic. A detection rule may identify repeated failed authentication, suspicious administrative changes, impossible or unusual sign-in behavior, endpoint alerts, or a combination of signals. The analyst then adds context rather than treating every alert as an incident.

The SOC also needs to monitor collection health. If Harbor Point's firewall normally produces events continuously and then becomes silent, silence is information. The cause may be a failed connector, expired credential, network change, service outage, logging configuration change, or actual device failure. Beacon opens or escalates an exception, and the responsible party restores the flow.

Verification means seeing new events arrive with correct timestamps and expected fields. Simply restarting a collector is not verification. The ticket remains open until the monitoring capability is demonstrably restored. If visibility was absent for a meaningful period, Harbor Point and its providers determine whether additional review is necessary.

Retention and searchability also matter. An organization may technically collect logs but retain them for too little time to support its operational or evidence needs. Storage and licensing decisions should therefore be tied to the organization's documented requirements rather than chosen only by default vendor settings.

22.49 Vulnerability Management: From Scanner to Remediation Program

A vulnerability scanner identifies conditions that may expose systems to known weaknesses. The scanner itself does not remediate the weakness and does not determine business priority in isolation. A mature program knows what assets should be scanned, whether authenticated or agent-based assessment is required, how frequently assessment occurs, how failures are detected, and how findings become owned work.

NorthStar begins by reconciling the vulnerability platform with Harbor Point's asset inventory. A workstation missing from the scanner is a coverage exception before anyone discusses the vulnerability findings on the other machines. The team then reviews findings, validates material issues, considers exposure and business context, assigns remediation, and tracks the result.

Suppose a critical vulnerability appears on an Internet-facing service and on an isolated laboratory system. The technical severity may be the same, but the exposure

and urgency can differ. The team considers exploitability, external reachability, asset importance, information handled, compensating protections, active exploitation intelligence, and the operational effect of remediation. Prioritization is disciplined risk treatment, not a method for making uncomfortable findings disappear.

After remediation, verification matters. If a configuration change was required, the team confirms the new configuration. If a patch was required, the team confirms the installed version and rescans or otherwise validates the result. Closure occurs when the intended security outcome is demonstrated, not when a technician marks a task complete.

22.50 Patch Management as an Exception-Driven Operation

Patch management is often described as deploying updates, but the operational challenge is managing the systems that do not follow the happy path. A mature program identifies applicable updates, tests where appropriate, schedules deployment, handles reboot requirements, monitors installation, investigates failures, manages approved exceptions, and verifies completion.

Consider one hundred Harbor Point workstations. Ninety-eight install a critical update successfully. A dashboard showing 98 percent may appear impressive, but the remaining two devices could be the Chief Engineer's laptop and an Internet-exposed administrative workstation. Percentages should therefore lead to exception lists, not replace them.

One failed device may lack disk space. Another may have a corrupted update component. A third may be offline because an employee is traveling. Each requires a different response. NorthStar's patch process should drive those exceptions to resolution or documented handling rather than repeatedly attempting the same failed installation without investigation.

The same principle applies to firmware, network appliances, hypervisors, security agents, and applications. The technology stack is larger than Windows Update. The organization should know which classes of technology have patch or update responsibility and who owns each class.

22.51 Backup Architecture, Restore Testing, and Ransomware Resilience

Backup design begins with recovery requirements. Harbor Point should know which systems and data must be recoverable, how much data loss can be tolerated, how quickly important services need to return, and which dependencies must be restored

together. Those business requirements influence backup frequency, retention, replication, recovery architecture, and testing.

A backup job can succeed while the organization remains unprotected. The most common reason is population failure: the system that matters was never included. A new engineering server may be created outside the normal provisioning process. Every configured backup job remains green because the backup platform does not know the server exists. Reconciliation between authoritative inventory and backup coverage detects the omission.

Restore testing should be realistic. Restoring a file demonstrates file recovery. Restoring a virtual machine demonstrates something more. Restoring an engineering application may require the application server, database, license service, identity dependency, configuration, and network access. The organization should test the level of recovery that matters to the business.

Ransomware resilience also requires thinking about administrative paths. If the same administrator account can modify production, disable endpoint security, and delete every backup, compromise of that identity creates a catastrophic common failure path. Backup administration may therefore require stronger separation, protected credentials, immutable or deletion-resistant storage capabilities where appropriate, and monitoring of destructive administrative actions.

22.52 Network Security and Firewall Operations in Practice

Network controls determine which systems can communicate and under what conditions. The goal is not to create complexity for its own sake. It is to reduce unnecessary communication paths and make permitted paths understandable. Segmentation can separate user devices, servers, management systems, guest networks, printers, specialized equipment, and other zones according to business and security requirements.

Suppose Harbor Point installs a new engineering application. The application vendor asks for 'all outbound Internet access' because that is easier to support. NorthStar should translate that request into actual technical requirements. Which destination services are required? Which protocols and ports? Does every workstation require the access or only the application server? Is inbound connectivity required? Can the destination be restricted? What logging will show use of the rule?

After implementation, the application is tested. NorthStar also tests that unintended communication has not been introduced. The ticket records the approved requirement and the firewall configuration records the technical implementation. Later, when the

application is retired, the associated rules should be reviewed and removed. Firewall governance therefore has a lifecycle just like software.

22.53 Secure Remote Administration Across Customers

An MSP's remote-access architecture should make customer context obvious and cross-customer mistakes difficult. Technician roles, customer containers, naming conventions, session banners, privileged-access workflows, and ticket integrations can all help. The design should not depend entirely on a technician remembering which browser tab is active.

Maria may see a server named FS01 at both Harbor Point and Falcon. Before executing a command, she verifies the customer, asset, ticket, and intended action. High-impact changes may require additional confirmation or peer review. Automation should include explicit customer targeting and safeguards against accidental broad execution.

Session accountability is equally important. Shared accounts make it difficult to determine which person performed an action. Individual identities and controlled elevation preserve attribution. When a technician leaves NorthStar, access removal can then be targeted to that individual instead of forcing a disruptive shared-password change across customers.

22.54 Software Control, SaaS, Browser Extensions, and AI in Detail

Modern software control extends far beyond traditional installed executables. A user can add a browser extension in seconds, authorize a SaaS application with an OAuth consent screen, upload a file to an online converter, connect a productivity application to cloud storage, or paste information into an AI service. Each action can create a new information path without installing a conventional application.

Harbor Point therefore needs an approval model based on function and information. A PDF utility that works entirely offline presents a different architecture from a web service that uploads every document to an external provider. An AI assistant integrated into an approved enterprise environment may have a different risk and contractual posture from a public consumer AI service. The organization should evaluate the actual service, configuration, information flow, terms, and technical controls rather than approve or reject a technology category by name alone.

Suppose Daniel discovers a free web tool that converts an engineering drawing into another format. The tool works beautifully. If Daniel uploads CUI, however, Harbor Point has created an external information flow. Before approving such a service, the

organization would need to understand where the information goes, how it is protected, whether the provider is appropriate for that information, what contractual terms apply, how long data is retained, whether administrators can control use, and what evidence exists.

Ownership continues after approval. Someone must monitor licensing, vendor notices, security advisories, configuration, integrations, and eventual retirement. Approval without ownership creates abandoned technology.

22.55 API and Service-Account Security

Human identities are only part of the environment. Applications authenticate to one another through service accounts, application registrations, certificates, secrets, managed identities, API tokens, and OAuth grants. These machine identities may operate continuously and may possess permissions broader than an ordinary user.

An integration should therefore have a documented purpose, owner, permissions, authentication method, credential lifecycle, data flow, and failure-detection mechanism. Secrets should not be embedded casually in scripts or tickets. Where the platform supports stronger certificate-based or managed authentication approaches, the architecture should evaluate them rather than defaulting to long-lived shared secrets.

Consider a reporting application authorized during a pilot. The pilot ends, but the application registration remains with permission to read directory information. Two years later nobody recognizes the name. A periodic application-permission review identifies it. The owner confirms that it is no longer required, and the authorization is removed through controlled change. This is the machine-identity equivalent of offboarding a former employee.

22.56 Microsoft Government Cloud: Begin With the Contract and Data

Harbor Point should not select GCC High simply because somebody says that 'CMMC means GCC High.' The decision begins with the contracts, information, regulatory obligations, eligibility, collaboration needs, and technical architecture. Microsoft currently describes GCC High as serving U.S. Government requirements including contractors holding or processing DoD CUI or subject to ITAR, and organizations go through an eligibility-validation process before an environment is established.

The contractor should work with appropriate contracting, legal, compliance, and technical expertise to understand what its agreements require. NorthStar can explain the technical differences and operational consequences. A readiness specialist can help map requirements and scope. A Microsoft Government Cloud implementation provider can design and execute the tenant and migration work. Those functions should cooperate without pretending that one discipline automatically replaces the others.

The selection also affects cost and operations. Third-party products that work in commercial Microsoft 365 may not support GCC High. Features may differ. Endpoints differ. Device migration can require re-enrollment. Support procedures can differ. The correct cloud is therefore a requirements decision with architectural consequences, not a prestige tier.

22.57 GCC High Tenant Implementation - A Detailed Walkthrough

After requirements and eligibility are addressed, the implementation team develops the target architecture. It inventories users, mailboxes, groups, shared mailboxes, Teams, SharePoint sites, OneDrive data, domains, DNS records, devices, administrators, service accounts, application registrations, mail relays, scanners, security tools, backup services, single-sign-on integrations, scripts, and external collaborators. Discovery is intentionally broad because the most disruptive migration problem is often a dependency nobody remembered.

The new tenant is established through the appropriate Microsoft Government licensing and provisioning process. Administrative identities are created and protected before broad user migration begins. The team defines long-term administrative roles and distinguishes them from temporary migration privileges. MFA and access policies are configured and tested. Emergency-access procedures are established according to the organization's design rather than invented during the first lockout.

Domains are validated and the DNS transition is planned. Email routing, autodiscover behavior, authentication, and other Microsoft 365 service dependencies are tested. The migration plan identifies which records change, when they change, how rollback would work where possible, and how the team will distinguish normal propagation delay from a configuration error.

Exchange, SharePoint, OneDrive, and Teams are configured according to the approved collaboration architecture. The team reviews legacy permissions instead of blindly copying every historical entitlement. A SharePoint site with thirty members

may need only eight current members. Migration fidelity is not the same as security correctness.

Device management receives its own workstream. Microsoft currently documents that GCC High and DoD use the government Intune service instance and that devices moving from commercial Intune to the government environment must unenroll and re-enroll because there is no built-in migration path. The team therefore creates a device-by-device transition plan, including remote users, failed enrollments, policy deployment, application deployment, endpoint-security continuity, and final reconciliation.

Network connectivity is validated against Microsoft's published GCC High endpoints. A user who can launch Word but cannot authenticate to a government service may have a network-path problem rather than an application-installation problem. Firewalls, proxies, filtering, and TLS inspection can therefore become part of Microsoft 365 troubleshooting.

Third-party integrations are tested individually. Microsoft Graph uses the worldwide graph.microsoft.com endpoint for GCC, while GCC High uses graph.microsoft.us. An application written only for the worldwide endpoint may fail even with correct credentials. The team verifies each backup, security, reporting, SSO, email, automation, and API integration against the actual national cloud rather than accepting the statement that a vendor 'supports Microsoft 365.'

22.58 GCC High Endpoint Build - What Happens on the Computer

Although GCC High itself is a cloud environment rather than a software package installed on a workstation, the endpoint still requires substantial technical work. Microsoft 365 client applications may be installed or reconfigured, the device establishes the appropriate identity relationship, device management is enrolled, security policies are applied, endpoint protection is validated, and approved applications and certificates are deployed according to the architecture.

Consider Daniel's laptop during migration. Before the change, NorthStar records the device state and confirms that required business data is protected. The old management relationship is removed at the planned point. The device is enrolled into the target government management environment. The technician verifies that the device appears under the correct identity, receives the expected configuration profiles, meets compliance conditions, and can reach required government-cloud services.

Endpoint protection is checked separately. The fact that Intune enrollment succeeded does not prove that EDR is healthy. The RMM agent is checked separately. The fact that RMM works does not prove that vulnerability management has discovered the machine. Each service is validated and the device is reconciled against the expected security stack.

Daniel then performs a user acceptance test: sign in, complete MFA, open Outlook, send and receive mail, access approved Teams and SharePoint resources, synchronize appropriate OneDrive content, use required engineering applications, and confirm that prohibited access from an unmanaged context behaves as designed. The implementation team records exceptions rather than declaring the migration successful because the desktop looks normal.

22.59 GCC High Operational Acceptance and Handoff

Technical implementation ends only after the continuing operators can maintain the environment. Harbor Point and NorthStar therefore perform an Operational Acceptance Test. An administrator creates a test identity through the approved workflow, assigns licensing, establishes authentication, grants approved group membership, enrolls a test endpoint, confirms policy and endpoint protection, locates audit information, and demonstrates how an access problem would be investigated.

The implementation provider then introduces controlled problems. A test device becomes noncompliant. An account fails authentication. A connector is disabled in a test context. The continuing administrators identify the symptoms, locate the relevant consoles and logs, follow escalation procedures, and explain when they would contact Microsoft or the implementation specialist. The objective is to expose knowledge gaps before the specialist leaves.

Handoff documentation includes tenant architecture, domains and DNS, administrative identities and roles, licensing, Entra configuration, MFA and Conditional Access, Exchange, Teams, SharePoint, OneDrive, Intune, Defender or other endpoint security, network endpoints, application registrations, APIs, third-party integrations, migration records, exceptions, diagrams, recovery information, and unresolved issues. Credentials and secrets are transferred through approved secure mechanisms rather than ordinary documents.

Temporary migration privileges are reviewed. Old tenant access is removed or retained only where there is a documented transition requirement. Legacy integrations are disabled when no longer needed. The final population is reconciled. Harbor Point formally understands who now owns identity administration, device

management, endpoint security, collaboration governance, integrations, monitoring, evidence, and escalation.

22.60 Maintaining GCC High After the Consultants Leave

Monday morning after handoff is where operational maturity becomes visible. A new employee needs an account. Another employee replaces a phone. A laptop fails enrollment. A guest needs temporary access. Microsoft announces a service change. An API certificate approaches expiration. A security alert appears. The environment is no longer an implementation project; it is a living production system.

Identity maintenance includes onboarding, termination, role changes, guest review, privileged-role review, MFA recovery, Conditional Access exceptions, and investigation of suspicious sign-ins. Device maintenance includes enrollment, compliance, configuration deployment, failed policy remediation, lost devices, replacement devices, stale records, and reconciliation with inventory.

Collaboration maintenance includes Teams ownership, guest access, SharePoint permissions, external sharing, abandoned sites, OneDrive lifecycle, and project closure. Security maintenance includes endpoint health, alert handling, vulnerability remediation, patching, log collection, integration health, and evidence retention.

Service-change management is also important. Microsoft cloud services evolve. The administrator should monitor changes relevant to the environment, determine whether they affect configuration or integrations, test material changes where appropriate, update documentation, and communicate operational impact. Continuous readiness depends on the environment and its documentation remaining synchronized.

22.61 Evidence Walkthrough - Proving a New User Was Properly Onboarded

An assessor or internal reviewer may ask how Harbor Point ensures that new employees receive only approved access and use managed devices. A weak answer is to display the onboarding policy. A stronger answer connects policy to operation.

Priya's manager submits an authorized onboarding request defining her role and required project access. The ticket records the request and approval. The identity platform records account creation. Group membership reflects the authorized role. MFA registration and sign-in records demonstrate authentication. Device inventory identifies the assigned laptop. Intune or the applicable management platform shows enrollment and policy state. EDR shows the endpoint protected. RMM shows

management coverage. Vulnerability management shows the device entering assessment. The ticket records validation.

The organization does not need every possible artifact for every question. It needs enough reliable evidence to demonstrate the process and the relevant assessment objectives. The strength comes from consistency between written procedure, actual configuration, operational records, and sampled results.

22.62 Evidence Walkthrough - Proving a Terminated User Lost Access

Offboarding demonstrates whether the organization can reverse authority. Human Resources or the authorized manager initiates the event. The identity is disabled according to procedure. Privileged roles and group memberships are removed. Remote-access mechanisms are addressed. Assigned devices are recovered or otherwise controlled. Third-party applications and customer-specific portals are reviewed when relevant.

The evidence may include the termination request, ticket chronology, identity disablement record, administrative logs, asset return record, and verification of removal from applicable systems. The exact evidence depends on the environment, but the narrative should be coherent: an authorized event occurred, defined actions followed, and the organization verified the result.

An MSP must pay special attention to technician offboarding because one technician may have access to many customer environments. NorthStar's offboarding checklist should therefore include its own identity provider, RMM, PSA, documentation, vault, security platforms, backup consoles, customer VPNs, cloud portals, API tokens, vendor portals, and any direct customer accounts.

22.63 Failure Laboratory - When the Backup Dashboard Lies by Omission

Harbor Point creates ENG-SRV-07 for a new engineering project. The server is added to inventory and RMM, but the engineer who built it forgets the backup-enrollment step. Every existing backup job succeeds overnight. The backup dashboard is entirely green.

Three weeks later, reconciliation compares production servers with the backup-protected population. ENG-SRV-07 is missing. NorthStar opens an exception, determines whether important data already exists on the server, adds the server to the

approved protection policy, performs an initial backup, and schedules a restore validation appropriate to the service.

The lesson is that dashboard health answers only the question the dashboard knows how to answer. It cannot report a failed backup job for a server it was never told to protect. Independent population reconciliation closes that gap.

22.64 Failure Laboratory - When the SIEM Goes Quiet

Beacon normally receives thousands of events each day from Harbor Point's firewall. At 10:14 a.m. the events stop. There is no attack alert because there are no events to analyze. A source-health rule identifies that the expected stream has become stale.

Beacon opens an escalation. NorthStar checks the firewall and discovers that a certificate used by the log-forwarding integration expired after an undocumented renewal process failed. NorthStar renews or replaces the credential through the approved procedure, restores forwarding, and confirms that fresh events arrive with correct timestamps and fields.

The team then asks a second question: why was the certificate expiration not managed before failure? The corrective action may include adding the certificate to a lifecycle inventory, assigning an owner, and creating advance expiration monitoring. Good incident handling fixes the immediate symptom and reduces the likelihood of recurrence.

22.65 Failure Laboratory - When a Patch Says Success but the Vulnerability Remains

NorthStar deploys an update to a Harbor Point server. The patch platform reports success. A subsequent vulnerability scan still detects the weakness. The technician should not dismiss the scanner automatically or assume the patch platform is wrong.

Investigation may reveal that the vulnerable application requires a separate component update, that a reboot is pending, that the scanner is detecting an old file, that the patch applied to one instance but not another, or that the vulnerability requires a configuration change in addition to the software update. The team examines the evidence and verifies the actual condition.

This example reinforces a central operating principle: action records and outcome records answer different questions. The patch system can prove an installation action. Verification demonstrates whether the intended security state was achieved.

22.66 Failure Laboratory - The Wrong-Customer Automation

Maria prepares a script to remove obsolete software from Falcon systems. The script is correct. The testing is correct. The mistake occurs during targeting: she selects a group that also contains Harbor Point devices.

A mature RMM design attempts to prevent this error before execution through customer segmentation, role restrictions, clear naming, scoped automation, peer review for high-impact jobs, and confirmation of the target population. If the error still occurs, logging should make the affected devices identifiable and the rollback or recovery process should be available.

The post-incident review should not stop with 'Maria needs to be more careful.' Human attention is important, but system design should reduce the probability and impact of predictable human mistakes.

22.67 Failure Laboratory - The Former Technician Who Still Has Access

Robert leaves NorthStar on Friday. His corporate Microsoft account is disabled immediately. On Monday, an audit discovers that Robert still has a direct local account on a customer's firewall and a separately issued account in a backup portal.

This is a failure of access inventory and offboarding design. NorthStar should know which systems can grant authority outside its central identity provider. Where possible, centralized identity and federated access reduce the number of independent accounts. Where direct accounts remain necessary, the offboarding workflow must include them.

The correction removes Robert's remaining access, reviews recent activity, determines whether credentials or tokens require rotation, and updates the access inventory. The deeper improvement is to make future offboarding verifiable rather than dependent on individual memory.

22.68 Failure Laboratory - GCC High Integration Breaks

NorthStar uses a commercial reporting application that authenticates successfully to ordinary Microsoft 365 customers. During Harbor Point's GCC High implementation, the same integration repeatedly fails. The technician initially suspects permissions and recreates the application registration.

The real problem is national-cloud support. Microsoft Graph for GCC High uses graph.microsoft.us rather than the worldwide graph.microsoft.com endpoint. The

vendor's application is hard-coded to the worldwide service. Correct credentials cannot solve an architectural incompatibility.

NorthStar records the requirement, contacts the vendor, and determines whether a supported government-cloud configuration exists. If not, Harbor Point and NorthStar choose an alternative approach rather than weakening the environment to make an incompatible tool work. Vendor compatibility becomes part of the technology-selection process for future customers.

22.69 Failure Laboratory - Firewall Troubleshooting Creates a Security Hole

An engineer reports that a new application cannot connect. Under pressure, a technician creates a temporary any-to-any rule to prove that the firewall is the problem. The application immediately works. The technician becomes distracted by another emergency and never removes the rule.

Months later, a firewall review discovers the temporary rule. The original troubleshooting step was understandable; the failure was lifecycle control. Temporary changes should have explicit scope, owner, ticket, expiration or review point, and validation. Automation can help identify rules containing temporary labels or rules that exceed an approved age.

The lesson applies beyond firewalls. Temporary administrator roles, temporary MFA exclusions, temporary guest accounts, temporary software, and temporary API permissions all have a tendency to become permanent unless the process contains a mechanism for revisiting them.

22.70 The Contractor-MSP-SOC Daily Operating Loop

Harbor Point, NorthStar, and Beacon should be able to describe how an ordinary day works. Harbor Point authorizes business access and communicates staffing, project, and system changes. NorthStar administers assigned technology and resolves management exceptions. Beacon monitors assigned security telemetry and escalates suspicious activity. Each party produces records through normal work.

During the day, automated systems generate health information. Devices check in. EDR reports protection status. Vulnerability tools collect results. Backup jobs complete. SIEM sources send events. RMM monitors services. Ticket queues receive failures. Technicians and analysts investigate exceptions rather than staring continuously at green dashboards.

At the end of the operating loop, the environment should be closer to its intended state than it was at the beginning. New assets have entered management, departed users have lost access, failures have owners, critical alerts have been investigated, changes are documented, and unresolved risks remain visible rather than disappearing into email.

22.71 Weekly and Monthly Technology-Stack Review

Daily operations handle immediate events. Periodic review looks for patterns and drift that individual tickets may not reveal. NorthStar and Harbor Point can review asset reconciliation, stale agents, vulnerability aging, patch exceptions, backup coverage, restore tests, privileged access, guest accounts, failed integrations, major changes, security incidents, and documentation updates.

The purpose is not to create a ceremonial meeting. It is to ask whether the security system remains coherent. If the asset inventory grows by fifteen devices while EDR grows by twelve, why? If vulnerability exceptions increase every month, is remediation capacity adequate? If the same backup job fails repeatedly, is the root cause being addressed? If privileged-role membership expands, do all assignments remain necessary?

Trend review turns operational data into management information. It also helps the contractor understand the MSP's work and helps the MSP identify where customer decisions or resources are blocking remediation.

22.72 The Random Tuesday Test - Expanded

Imagine that no assessor is scheduled and nobody has spent the previous month cleaning records. At 10:00 a.m. on an ordinary Tuesday, Harbor Point asks NorthStar to demonstrate the current state of the environment.

Can the parties produce the authoritative device population? Can they show which devices are missing EDR, vulnerability, management, or backup coverage? Can they identify current privileged administrators and explain why each has access? Can Beacon show the expected log sources and identify any stale source? Can NorthStar show unresolved critical vulnerabilities and the owner of each exception? Can Harbor Point show recent onboarding and offboarding samples? Can the team retrieve evidence of a recent firewall change and explain who authorized it?

If those answers exist because the systems and workflows create them every day, readiness is operational. If the answers require spreadsheets to be reconstructed from memory, screenshots to be staged, and technicians to search old email, the

organization has identified a readiness gap even if the underlying technology is sophisticated.

22.73 Closing - What a CMMC-Ready Technology Stack Really Means

The most important conclusion of this chapter is that CMMC readiness cannot be purchased as a bundle of products. A defense contractor can buy excellent technology and still operate it poorly. An MSP can deploy powerful tools and still fail to define responsibility. A SOC can receive millions of events and still miss the one source that stopped reporting. A backup platform can show green while an important server was never enrolled.

A mature technology stack connects requirements to architecture, architecture to implementation, implementation to operation, operation to evidence, and evidence back to validation. The contractor understands what it owns. The MSP understands what it operates. External providers understand their assigned functions. Technicians know how to detect and repair failures. Managers can see unresolved exceptions. Documentation follows meaningful change.

The goal is not a perfect environment in which nothing ever fails. Real systems fail. Agents stop reporting. patches fail, users make mistakes, integrations break, vendors change services, and administrators leave. The goal is an environment in which failure becomes visible, ownership is clear, corrective action is controlled, verification occurs, and evidence remains.

Normal operations should create security. Normal operations should create evidence. Normal operations should maintain readiness. That operating principle is the bridge from the technology stack in this chapter to Chapter 23, where the book turns to maintaining certification and continuous readiness over time.

Current Authoritative Microsoft References Used for This Edition

Microsoft Learn - Office 365 US Government Service Descriptions: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-us-government/office-365-us-government

Microsoft Learn - Office 365 GCC High and DoD: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-us-government/gcc-high-and-dod

Microsoft Learn - Microsoft Graph National Cloud Deployments: https://learn.microsoft.com/en-us/graph/deployments

Microsoft Learn - Microsoft Intune Government Service Overview: https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/intune-govt-service-description

Microsoft Learn - Microsoft 365 U.S. Government GCC High Endpoints: https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-u-s-government-gcc-high-endpoints

These cloud-service facts are time-sensitive. They should be revalidated against the current Microsoft service descriptions during final whole-book production and in future editions.

Chapter 22 Deep Teaching Expansion: The Why Before the How

A beginner cannot retain a procedure if the reason for the procedure is unclear. For that reason, this section revisits the major components of the CMMC-ready technology stack from a different direction. Each topic begins with the problem that exists before the technology is introduced, explains why the problem matters to a defense contractor and an MSP, describes what could happen if the problem is ignored, and only then moves into implementation, operation, failure, troubleshooting, verification, and evidence. The purpose is not to repeat product descriptions. It is to give the reader a mental model that explains why the technology belongs in the architecture.

This distinction is especially important in CMMC work because organizations can easily become focused on buying tools. A tool is useful only when it performs a needed security function inside a defined operating process. The contractor must understand the business and information risk. The MSP must understand the operational responsibility. The technician must understand the implementation. The assessor ultimately needs evidence that the required security outcome is actually occurring. Those four perspectives should reinforce one another.

22.74 Why Asset Inventory Comes Before Security Tooling

Before an organization can protect systems, it must know which systems exist. This sounds obvious, but modern environments create assets in many ways. A laptop may be purchased by IT, a virtual server may be created by an engineer, a cloud workload may be provisioned by a vendor, a mobile device may be enrolled by a user, and a temporary test system may quietly become permanent. If those assets enter the environment without entering the organization's management process, security controls can miss them.

The reason inventory matters is therefore not administrative neatness. Inventory defines the population against which security expectations are measured. If Harbor Point says every managed workstation must have EDR, the phrase 'every managed workstation' must refer to a known population. Without that population, a report showing 100 percent EDR coverage can be misleading because the report can only count devices the EDR platform already knows about.

The same logic applies to vulnerability scanning, patching, encryption, backup, configuration management, and offboarding. A forgotten asset can become a forgotten vulnerability, an unpatched operating system, an unprotected repository of CUI, or an unmanaged path into the environment. The asset inventory therefore

becomes the common reference that allows Harbor Point and NorthStar to ask whether each required protection has actually reached the systems it is supposed to protect.

Implementation begins by defining authoritative sources and lifecycle events. Procurement, provisioning, assignment, virtual-machine creation, cloud-resource creation, rebuild, transfer, and retirement should update the asset record. Operations then reconcile that record against security platforms. Evidence is not merely the inventory itself; it is the repeatable process showing that discrepancies are detected, investigated, corrected, and verified.

22.75 Why Antivirus Alone Is Not Enough

Traditional antivirus was designed primarily to recognize known malicious software, often through signatures and other detection techniques. That remains useful, but modern attacks frequently use legitimate tools, scripts, stolen credentials, living-off-the-land techniques, memory-resident behavior, and sequences of actions that may not look like a single malicious file. A defense contractor therefore needs more than the question 'Did antivirus find a virus?'

EDR exists because defenders need visibility into what an endpoint is doing before, during, and after suspicious activity. The security team may need to know which process launched another process, which account was active, what network connection followed, what file changed, whether persistence was created, and whether the same behavior appeared elsewhere. This context allows an analyst to investigate behavior rather than waiting for a known malware signature.

This does not mean EDR magically prevents every attack. It can be misconfigured, disabled, unhealthy, overwhelmed by exclusions, or absent from a device. That is why Harbor Point must care about both protection capability and coverage. NorthStar may operate the agents while Beacon investigates alerts, but somebody must verify that the expected endpoints are actually reporting.

When Daniel opens a malicious attachment, antivirus might recognize a known payload and block it immediately. If the attacker instead abuses a legitimate scripting engine, EDR may provide the behavioral context needed to detect and investigate the sequence. The why behind EDR is therefore visibility and response depth, while the how includes deployment, policy, health monitoring, alert handling, isolation, remediation, and evidence.

22.76 Why RMM and EDR Are Different Even Though Both Have Agents

A new MSP technician may reasonably ask why a customer needs both RMM and EDR when both products install agents and both can report information about a computer. The answer is that they exist for different primary purposes. RMM is principally an administration and operations platform. EDR is principally a security detection, investigation, and response platform.

NorthStar uses RMM to manage devices at scale: inventory, service monitoring, remote support, scripting, software deployment, maintenance, and other administrative functions. Beacon and NorthStar use EDR to understand potentially malicious endpoint behavior and support security response. There can be overlapping features, but overlap does not make the functions identical.

This separation also provides useful independent evidence. If RMM says a device exists but EDR does not, the disagreement is important. If both functions were treated as one undifferentiated tool, the organization could lose the ability to identify a missing security control. Reconciliation between independent systems is valuable precisely because the systems answer different questions.

The operational lesson is not that every organization must buy two particular products. It is that the required functions must be covered. If one platform legitimately provides multiple functions, the organization should still understand how each function is configured, monitored, evidenced, and protected from common failure.

22.77 Why MFA Exists and Why Passwords Are Not Enough

A password is a reusable secret. The user knows it, types it, stores it in memory or a password manager, and may accidentally reveal it. Attackers can obtain passwords through phishing, credential-stealing malware, password reuse, database breaches, social engineering, or guessing. If possession of the password alone is enough to authenticate, stealing the password can become equivalent to stealing the user's digital identity.

MFA changes that equation by requiring another factor or stronger authentication mechanism in addition to, or instead of relying solely on, a password. The security value is not that MFA makes compromise impossible. The value is that one stolen secret is less likely to be sufficient by itself. This is particularly important for administrators because a compromised privileged account can affect many systems and security controls.

Harbor Point therefore should not think of MFA as a checkbox that becomes complete when a policy is switched on. It must ask which identities are covered, which are excluded, how administrators authenticate, how users recover from lost devices, how emergency access works, and whether legacy protocols or applications create alternate paths around the intended protection.

NorthStar's operational responsibility may include configuring policies and supporting registration, but Harbor Point still owns decisions about who should have access. Evidence can include policy configuration, identity populations, exception records, authentication logs, and sampled tests showing that expected scenarios require the intended authentication.

22.78 Why Conditional Access Is Needed When MFA Already Exists

MFA answers an important question: can the person provide stronger proof of identity? It does not necessarily answer whether the circumstances of the access request are acceptable. A legitimate employee can successfully complete MFA from a personal computer, an unmanaged device, an unexpected location, or a context the organization does not want to use for sensitive information.

Conditional Access exists to combine identity with additional conditions and policy decisions. Depending on the architecture and available capabilities, the organization can consider the user, role, application, device state, authentication strength, risk signals, location conditions, and other context. The purpose is to make access decisions that reflect both who is asking and the circumstances under which access is requested.

Daniel may be fully authorized to work with an engineering project. Harbor Point can still decide that access to the project's protected resources should occur only from managed devices that satisfy required security conditions. Daniel's business authorization remains valid; the personal computer simply does not satisfy the technical conditions for that access path.

The how therefore follows the why. Harbor Point defines the intended access model. NorthStar configures and tests policies. Exceptions are documented. Sign-in logs are reviewed. A test from the managed laptop should succeed when appropriate, while a test from an unmanaged device should produce the intended restriction. Evidence shows that the access model is not merely written but enforced.

22.79 Why Least Privilege Matters

Administrative privilege changes the consequences of a mistake or compromise. An ordinary account may be limited to the user's own resources, while a highly privileged account may create users, change access policies, disable security controls, modify configurations, or access many systems. The more authority an identity has, the larger the potential impact if that authority is misused.

Least privilege exists to reduce that impact. It does not mean making employees unable to do their jobs. It means providing the authority needed for the task without granting unrelated power merely for convenience. A help-desk technician who resets passwords does not automatically need global tenant administration. A backup operator does not automatically need firewall administration.

In an MSP, the problem becomes more serious because privilege can cross customer boundaries. Maria's ability to administer Harbor Point should not automatically grant the same authority over Meridian and Falcon. Customer separation, role design, individual identities, controlled elevation, and privileged-access workflows reduce the blast radius of both mistakes and compromise.

Operationally, NorthStar reviews roles when technicians join, change responsibilities, or leave. Harbor Point reviews its own privileged identities. Temporary implementation privileges receive expiration or review. Evidence includes role assignments, approvals, access reviews, elevation records, and administrative logs.

22.80 Why Centralized Logging and a SIEM Are Needed

Every major system creates its own view of activity. The identity provider knows about authentication. The firewall knows about network connections. EDR knows about endpoint behavior. Microsoft 365 knows about cloud activity. Servers know about local events. If each record remains isolated in a separate console, investigators must manually reconstruct events across many systems while an incident is unfolding.

A SIEM exists to bring relevant security information together so that events can be searched, correlated, retained, and analyzed in a common operational context. The value is not simply central storage. The value is the ability to connect signals. A suspicious login followed by unusual endpoint execution and an outbound connection may be much more meaningful together than any single event viewed alone.

The SIEM also creates a place to implement detection logic and measure source health. If Harbor Point expects firewall, identity, EDR, and server events, the

monitoring program can identify when one of those sources becomes stale. Without source-health monitoring, a failed connector can create a silent blind spot.

The how includes source inventory, connectors, parsing, time synchronization, detection rules, retention, access control, tuning, escalation, and verification. Evidence can demonstrate both security events and the health of the monitoring system itself.

22.81 Why a SOC Is Needed When the SIEM Already Generates Alerts

A SIEM can generate alerts, but an alert is not the same as an investigation. Security tools routinely produce events that require context. Some are benign. Some are misconfigurations. Some are genuine attacks. Someone must examine the evidence, decide what it means, determine urgency, and coordinate the next action.

A SOC provides that operational capability. Beacon's analysts monitor assigned telemetry, investigate alerts, enrich them with context, identify related activity, escalate according to Harbor Point's procedures, and preserve the investigation record. The SOC may use automation, but human or operational judgment remains necessary for many events.

This distinction matters contractually. Harbor Point should know whether Beacon merely forwards vendor alerts or actually performs triage and investigation. NorthStar should know when Beacon expects NorthStar to act. Beacon should know who receives an escalation after hours. A tool subscription cannot substitute for defining those responsibilities.

The evidence produced by the SOC includes alert records, analyst notes, escalation timestamps, related-event searches, and incident handoffs. Those records help demonstrate that monitoring is an operating process rather than a dashboard that nobody watches.

22.82 Why Vulnerability Management Is Needed When Patching Exists

Patching is one method of correcting weaknesses. Vulnerability management is the broader process of discovering, understanding, prioritizing, tracking, and verifying security weaknesses across the environment. Some vulnerabilities require patches, but others arise from insecure configuration, unsupported software, exposed services, weak protocols, application design, or missing hardening.

Windows Update therefore cannot answer the question 'What weaknesses exist in our environment?' It can answer a narrower question about applicable Microsoft updates on systems it manages. A vulnerability-management platform or process provides another perspective and can identify conditions that ordinary patch tooling does not address.

The program also creates prioritization. Harbor Point cannot treat every finding as identical. Exposure, exploitability, asset importance, CUI relevance, active exploitation, available mitigations, and operational constraints affect urgency. Prioritization should accelerate the most meaningful risk reduction without becoming a mechanism for indefinite delay.

Verification closes the loop. If NorthStar patches a system, the vulnerability platform can help demonstrate whether the weakness is actually gone. If it remains, the team investigates why. Evidence therefore includes discovery, assignment, remediation, exception handling, rescanning, and closure.

22.83 Why Patch Management Needs More Than Automatic Updates

Automatic updates are valuable, but they do not eliminate the need for patch management. Systems can be offline, updates can fail, reboots can remain pending, applications can require separate installers, firmware can be outside the operating-system update mechanism, and production systems may require testing or scheduled maintenance.

Patch management exists to turn available updates into a controlled operational outcome. The organization needs to know which systems require the update, which received it, which failed, which are pending restart, which are temporarily excepted, and whether the vulnerability or defect was actually resolved.

Harbor Point's 98 percent success rate is not the end of the story. NorthStar identifies the two failures and investigates them individually. One laptop may be traveling and offline; another server may have a corrupted component. The exceptions drive work until the intended state is achieved or a documented temporary treatment is approved.

This is why metrics should not stop at percentages. The important management question is often the identity and risk of the remaining exceptions. Evidence includes deployment records, failure tickets, exception approvals, verification results, and trend information.

22.84 Why Backup Is Needed Even When Data Is in Microsoft 365

Cloud services provide resilient infrastructure and service-level capabilities, but a defense contractor still needs to think about recovery from its own operational failures and business requirements. Users can delete information, permissions can be changed, ransomware or malicious actions can affect accessible data, retention settings can be misunderstood, and business recovery requirements may differ from the native recovery capabilities of a service.

The correct question is therefore not 'Does Microsoft back up Microsoft 365?' The useful question is 'What recovery outcomes does Harbor Point require, and which combination of Microsoft capabilities, retention configuration, versioning, recycle mechanisms, and any additional backup or recovery services satisfies those outcomes?' The answer depends on the service, licensing, configuration, contractual requirements, and business need.

This reasoning also prevents the opposite mistake of buying a third-party backup product automatically. Harbor Point should define recovery requirements first. If an additional product is selected, NorthStar must verify that it supports the actual government-cloud environment, protects the intended workloads, uses appropriate authentication, and does not create an inappropriate external data path.

Evidence includes recovery configuration, protected populations, job status where applicable, restore-test results, exception records, and documented recovery procedures. The ultimate why is business resilience: the organization must be able to recover the information and services it depends upon.

22.85 Why Restore Testing Is More Important Than a Green Backup Dashboard

A backup job proves that a backup process reported success. It does not prove that the organization can recover the business capability when needed. Files can be corrupt, dependencies can be missing, credentials can be unavailable, application versions can be incompatible, or the backup can omit a component nobody realized was necessary.

Restore testing exists because recovery is an outcome that must be demonstrated. Harbor Point may successfully restore an engineering application server only to discover that the associated database, license service, or configuration repository was not included in the recovery plan. The server is back, but the engineering capability is not.

A realistic test therefore begins with the business service and works backward to the technical dependencies. The test scope can vary, but the organization should know what it is proving. File recovery, mailbox recovery, database recovery, virtual-machine recovery, and full service recovery are different levels of assurance.

NorthStar documents the test, result, time required, failures encountered, corrective actions, and final verification. Those records improve the recovery design and provide evidence that backup is not merely configured but usable.

22.86 Why Network Segmentation Matters

A flat network assumes that systems that can reach the network may communicate broadly with one another. That may be convenient, but it increases the number of paths available to malware, compromised accounts, misconfigured devices, and unauthorized users. A single compromised workstation can potentially reach systems that have no business reason to communicate with it.

Segmentation reduces unnecessary paths. It can separate user workstations, servers, management systems, printers, guest devices, specialized equipment, and other classes of assets. The purpose is not to create arbitrary VLANs. The purpose is to make communication reflect business need and reduce the blast radius of compromise.

Harbor Point's printer may need to communicate with print services and approved scanning destinations. It does not need unrestricted access to every engineering server. By limiting communication, Harbor Point reduces what an attacker controlling that printer could reach and makes unusual traffic easier to identify.

The how includes network architecture, firewall rules, routing, access-control lists, wireless design, remote-access paths, monitoring, and change control. Evidence can include diagrams, rule sets, approved change tickets, configuration exports, and test results.

22.87 Why Change Control Is a Security Control

Security environments are not static. Administrators change firewall rules, add applications, create groups, modify Conditional Access, replace servers, and update integrations. Each change can improve the environment, break the environment, or unintentionally weaken a protection that previously worked.

Change control exists to connect technical change with purpose, authorization, impact analysis, testing, and documentation. It is not intended to prevent administrators from

working. It prevents important changes from becoming unexplained facts that future technicians inherit without context.

A temporary any-to-any firewall rule demonstrates the problem. The technician may create it for a valid troubleshooting reason. Without a ticket, owner, and expiration point, the temporary condition can survive for years. The security failure is not necessarily the original troubleshooting step; it is the absence of lifecycle control.

Evidence from change control explains why the environment looks the way it does. A configuration export proves what exists. A change record explains why it exists, who approved it, who implemented it, how it was tested, and when it should be reviewed.

22.88 Why Ticketing Matters to CMMC Operations

A technician can fix a problem without a ticket, but the organization then loses part of the institutional record. The next technician may not know why the change was made. Management may not know who authorized it. An assessor may see the technical result but not the operational process behind it.

Ticketing creates traceability. It connects the request, authorization, technician, asset, action, result, exception, and verification. In an MSP, it also creates customer context. Maria should know that the work belongs to Harbor Point, which procedure applies, and which approvals are required before she begins.

The ticket does not need to become a novel. It needs enough information to make the work understandable and reproducible. 'Fixed' does not explain what was wrong or how the result was verified. A useful closure note records the observed condition, action taken, validation, and any continuing risk or follow-up.

This is why PSA/ITSM belongs in the technology stack discussion. It may not block malware directly, but it governs how security-relevant work is authorized, executed, recorded, and evidenced.

22.89 Why Documentation Must Match Reality

Policies, procedures, diagrams, inventories, and the SSP describe how the organization says its environment works. If those documents drift away from reality, they can become dangerous because administrators and assessors make decisions based on an obsolete model.

Suppose Harbor Point's diagram shows three servers but a fourth production server was added six months ago. The new server may have different logging, backup, or network requirements that never entered the documented architecture. The problem is

not merely that the diagram is old. The discrepancy may reveal that the change process bypassed security review.

Documentation maintenance therefore follows meaningful change. New systems, new CUI flows, new external providers, new privileged pathways, major cloud changes, and significant security-control changes should trigger review of the relevant documentation. Periodic validation then catches changes that escaped the event-driven process.

Evidence of documentation quality includes revision history, approved changes, current diagrams, responsibility matrices, inventories, and sampled comparisons between documented and actual configuration. Documentation should describe the environment the organization operates, not the environment it remembers building.

22.90 Why Evidence Must Be Designed Into Operations

Organizations often begin collecting evidence shortly before an assessment. That creates pressure to reconstruct months of activity from screenshots, emails, and technician memory. The deeper problem is that the operating process was never designed to leave reliable records.

Evidence-by-design means asking during process design what record will demonstrate that the activity occurred. User onboarding naturally creates a request, approval, identity record, device record, and ticket. Patch management naturally creates deployment status and exception records. Vulnerability management creates findings and verification. Incident response creates alerts, investigation notes, actions, and closure.

The purpose is not to save everything forever. Evidence should support specific security and operational claims. The organization determines what it needs, where the authoritative record lives, who owns it, how long it remains available, and how it will be retrieved.

When normal operations create evidence automatically or consistently, assessment preparation becomes validation and organization rather than historical reconstruction. That is why evidence architecture is part of technology architecture.

22.91 Why Security Tools Themselves Need Security

Security tools frequently possess more authority than ordinary business applications. RMM can execute commands. EDR can isolate endpoints. Identity platforms can grant roles. Backup systems can restore or delete data. SIEM platforms can reveal

sensitive security information. Documentation systems can expose architecture and credentials.

An attacker who compromises one of these platforms may gain an efficient way to attack the environment. The organization should therefore protect the tools with strong authentication, least privilege, logging, patching, secure integrations, vendor-risk awareness, recovery planning, and monitoring of administrative actions.

This is another reason shared accounts are dangerous. If several technicians use one powerful account, unusual activity is harder to attribute and offboarding becomes disruptive. Individual identities and controlled elevation create accountability and reduce persistent privilege.

The why is simple: a security tool is not automatically secure because its purpose is security. Its own compromise can turn defensive capability into offensive capability.

22.92 Why MSP Customer Separation Matters

An MSP gains efficiency by managing many customers through shared operational platforms. That efficiency creates concentration risk. A mistake, compromised technician, poorly scoped script, or insecure integration can potentially affect more than one customer if boundaries are weak.

Customer separation exists to reduce that cross-customer blast radius. It includes logical tenant separation, role restrictions, customer-specific credentials, naming standards, ticket context, automation targeting, documentation permissions, and careful use of shared infrastructure.

Maria may legitimately support Harbor Point and Falcon, but a technician who supports only Meridian should not automatically see Harbor Point's systems. A script prepared for Falcon should not be able to reach Harbor Point because of a careless group selection. The platform design should reinforce customer boundaries rather than relying solely on human memory.

Evidence can include role assignments, tenant configuration, access reviews, audit logs, and controlled tests. The contractor also benefits from understanding how its MSP separates customer data and administrative authority.

22.93 Why Government Clouds Exist

Government cloud environments exist because some government and regulated workloads require commitments and architectures that differ from ordinary commercial cloud services. These can include U.S. data-location commitments,

personnel screening, government-specific compliance requirements, isolated national-cloud infrastructure, and service configurations designed for public-sector and defense needs.

Microsoft currently states that Office 365 Government customer content is logically segregated from commercial Office 365 customer content, stored within the United States, and subject to restricted access by screened Microsoft personnel. Microsoft describes GCC High and DoD as addressing additional Department of Defense and ITAR-related requirements. Those characteristics explain why a defense contractor may evaluate a government environment rather than treating commercial Microsoft 365 as automatically interchangeable.

The existence of a government cloud does not mean every defense contractor automatically needs the highest government offering. The organization must evaluate the actual contracts, information, eligibility, required service commitments, collaboration needs, and technical architecture. Cloud selection is therefore a requirements decision, not a status symbol.

This also explains why government cloud can cost more or require more specialized support. Separation, validation, different endpoints, feature differences, and a smaller ecosystem of compatible integrations can create operational consequences that must be planned.

22.94 Why GCC High Does Not Make an Organization CMMC Compliant

GCC High can provide cloud capabilities and service commitments that may be important to a contractor's architecture, but CMMC concerns the contractor's implementation of applicable security requirements across the assessed environment. Purchasing a cloud service cannot make business authorization decisions, maintain the contractor's asset inventory, remove a departed employee, configure every endpoint, manage every firewall, investigate every incident, or ensure that procedures are followed.

The cloud provider and contractor therefore have different responsibilities. Microsoft operates the service according to its service commitments. Harbor Point configures and uses the service within its own environment. NorthStar may administer assigned functions. Beacon may monitor assigned telemetry. The contractor remains responsible for understanding how those responsibilities combine.

This is why the phrase 'We have GCC High, so we are compliant' is dangerous. It confuses a component of the architecture with the complete security program. The

correct question is what security functions the cloud provides or supports, what the contractor must configure, what external providers perform, and what evidence demonstrates the resulting implementation.

The practical benefit of this explanation is that the reader can evaluate any provider the same way. A compliant or accredited service can contribute important capabilities without transferring all organizational accountability to the provider.

22.95 Why GCC and GCC High Integrations Behave Differently

National-cloud separation affects more than the address of a portal. Applications authenticate against cloud-specific identity services and call cloud-specific API endpoints. Microsoft currently documents that GCC continues to use worldwide Microsoft Graph endpoints, while GCC High uses the U.S. Government endpoint graph.microsoft.us and Azure Government identity endpoints.

This matters because software is often written with assumptions. A commercial reporting application may assume graph.microsoft.com, a commercial Azure portal, or a feature available only in the global cloud. Correct credentials cannot overcome an application that is pointed at the wrong national cloud or depends on an unsupported service.

NorthStar should therefore evaluate integrations before migration. The vendor should identify exact GCC High support, required endpoints, permissions, data flows, and feature limitations. Harbor Point should understand whether the integration sends information outside the government environment and whether that use is appropriate for the information involved.

Testing should include successful authentication, required API operations, error handling, monitoring, and credential lifecycle. The why behind this extra work is architectural isolation: the same separation that supports government-cloud requirements also means commercial assumptions cannot always cross the boundary.

22.96 Why Moving to GCC High Is a Migration Project, Not a License Change

A beginner may imagine that changing from commercial Microsoft 365 to GCC High is similar to upgrading a subscription. In reality, the government environment can involve a separate tenant, identity context, endpoints, service instances, integrations, and device-management relationships. Existing data and configurations must be discovered, mapped, migrated, recreated, or deliberately retired.

Microsoft's current Intune documentation is a concrete example. Devices moving from commercial Intune to the government cloud must unenroll from the current tenant and re-enroll in the new tenant; Microsoft states that there is no built-in migration between those service instances. That means the endpoint relationship itself must be transitioned rather than merely changing a license.

The same migration mindset applies to users, mail, collaboration sites, applications, DNS, groups, guests, scripts, APIs, and security integrations. The team needs a source state, target state, migration method, validation test, exception process, and rollback or recovery approach where appropriate.

The why behind formal migration planning is continuity. Harbor Point is changing infrastructure while employees still need to work and security controls still need to operate. The project must protect both business availability and security during the transition.

22.97 Why DNS Matters to Microsoft 365 Government

DNS is often invisible to end users, but it directs important service behavior. Domain validation, mail routing, service discovery, and other cloud functions depend on DNS records. A migration can be technically correct inside the tenant and still fail for users if the public DNS configuration points to the wrong destination.

This is why migration teams document existing records before making changes. They identify which records support mail, authentication, verification, and other services; plan the sequence of changes; consider propagation; and define validation tests. The objective is not merely to edit DNS but to preserve the intended service path.

During Harbor Point's cutover, a missing or incorrect record could cause mail-delivery problems that appear to be Exchange failures. Troubleshooting requires following the path rather than reinstalling client software. The technician checks DNS resolution, service endpoints, tenant configuration, authentication, and message flow in a logical order.

Evidence includes the approved change, before-and-after configuration, test results, and incident records if the cutover encounters problems. DNS matters because cloud services depend on external naming and routing decisions that exist outside the application interface.

22.98 Why Device Management Matters in a Cloud Environment

Moving applications and data to the cloud does not eliminate the endpoint. Users still read, create, download, synchronize, print, and transmit information from physical

devices. A compromised or unmanaged laptop can undermine strong cloud controls because the user interacts with the cloud through that endpoint.

Device management exists to establish and maintain an expected endpoint state. The organization can deploy configuration, require encryption, manage applications, evaluate compliance conditions, and maintain an inventory relationship between user, device, and policy. The exact capabilities depend on the platform and licensing, but the security purpose is consistent.

Harbor Point may require a managed device before Daniel can access a protected engineering resource. That decision connects Conditional Access with device management. If the device falls out of compliance, access can be restricted according to the architecture. The cloud and endpoint are therefore parts of one security system.

NorthStar's job does not end at enrollment. Failed policies, stale devices, replaced laptops, lost systems, and unenrolled endpoints become exceptions. Reconciliation and health monitoring show whether the management relationship remains effective.

22.99 Why Email and Collaboration Need Governance

Email, Teams, SharePoint, and OneDrive make collaboration easy, which is precisely why governance is needed. A user can create a group, invite a guest, share a link, synchronize files, forward a message, or create a new workspace with very little friction. Convenience can create information paths faster than administrators notice them.

Governance defines which capabilities are permitted, who can create them, how external access is approved, how project ownership is maintained, and what happens when the business purpose ends. The objective is not to stop collaboration. It is to make collaboration consistent with the organization's information-handling requirements.

A guest invited to a six-month project may still exist three years later because the technology has no knowledge of the business relationship unless a lifecycle process supplies that context. Periodic guest review and project-closeout procedures reconnect technical access with business need.

Evidence includes guest inventories, sharing configuration, approval records, access reviews, group ownership, and offboarding actions. The why is that collaboration systems are information-distribution systems, not merely productivity applications.

22.100 Why Secure File Exchange Needs Its Own Design

Organizations sometimes assume that encryption alone makes a transfer method appropriate. Encryption is important, but secure exchange also involves identity, recipient authorization, data location, retention, access control, logging, administrative responsibility, and the provider's suitability for the information.

Daniel may be sending CUI to an authorized subcontractor. That answers who should receive the information. It does not automatically answer whether a personal Dropbox account, consumer email service, public file-transfer site, or other ad hoc method is approved for that information.

Harbor Point therefore defines approved exchange methods and teaches users when to use them. NorthStar may configure the technical service, identity integration, sharing controls, and monitoring. The contractor still determines the business relationship and information-handling rules.

The evidence can include approved-service configuration, access records, transfer logs where available, user authorization, and procedures. The why is to control the entire information path rather than only the sender and recipient.

22.101 Why AI Governance Belongs in the Technology Stack

AI services can receive prompts, documents, source code, images, meeting content, and other information. They can also appear inside products that users already trust. This creates a new information path that may not look like traditional file transfer because the user experiences it as asking a question or requesting assistance.

The security issue is therefore not whether AI is good or bad. The issue is what information is being provided, to which service, under what account and contractual terms, with what retention and processing behavior, and whether that use is approved for the information involved.

Harbor Point can allow approved AI use for appropriate information while restricting CUI from unapproved services. NorthStar can support technical enforcement where feasible, but the contractor must define the business policy. Training matters because users need to recognize that pasting text into a prompt is still transmitting information.

Evidence can include approved-service lists, policy, technical restrictions, training, application configuration, and investigation records. The why is information governance: AI changes how easily information can leave an approved boundary.

22.102 Why APIs and Service Accounts Are Identities

Applications need authority to communicate with other applications. They obtain that authority through service accounts, application registrations, API keys, OAuth grants, certificates, managed identities, and other mechanisms. These are identities even though no human types a password every morning.

The risk can be substantial because machine identities often run continuously and may possess broad permissions. A forgotten API token can outlive the project that created it. A hard-coded secret can be copied into source code or tickets. An overprivileged application can expose more information than its business function requires.

The organization should therefore manage machine identities with the same seriousness as human identities: owner, purpose, least privilege, credential lifecycle, monitoring, and offboarding. Where possible, stronger mechanisms that reduce long-lived secrets should be considered within the supported architecture.

NorthStar's periodic integration review asks whether each application is still needed and whether its permissions remain appropriate. Evidence includes application inventories, permission reviews, credential-rotation records, and controlled removal of obsolete integrations.

22.103 Why Security Exceptions Need Owners and Expiration

Real environments cannot always reach the desired state immediately. A legacy application may prevent a patch, a business partner may require temporary access, a device may be offline, or a migration may require a temporary policy exception. Pretending exceptions never exist encourages administrators to hide them.

A controlled exception makes the deviation visible. It records what differs from the intended state, why, who owns the issue, what risk or exposure exists, what temporary protections are used, what permanent resolution is planned, and when the exception must be reviewed.

Expiration or review is essential because temporary conditions naturally become permanent. The three-year MFA exclusion and the forgotten firewall rule are examples of the same organizational failure: nobody was forced to reconsider a once-valid decision.

Evidence includes the exception record, approval, compensating actions, review history, and closure. The why is not bureaucracy; it is preventing known deviations from disappearing into the background.

22.104 Why Reconciliation Is More Powerful Than a Dashboard

Dashboards summarize what a product knows. They cannot easily reveal what the product does not know. An EDR dashboard can report that all registered agents are healthy while a newly built computer that never received the agent remains completely absent.

Reconciliation compares independent populations to find omissions. Inventory versus EDR asks whether every expected device is protected. Inventory versus backup asks whether every expected system is recoverable. Identity versus privileged-access records asks whether all administrators are known. Expected log sources versus SIEM activity asks whether monitoring coverage remains complete.

The differences become the work queue. NorthStar does not need to panic because two lists differ; it needs to explain every meaningful difference. Some will be legitimate. Others will expose failed agents, stale records, unmanaged assets, or process gaps.

The why is epistemic: reconciliation helps the organization discover what a single system cannot tell it about itself. It is one of the strongest ways to detect silent control failure.

22.105 Why the MSP Cannot Simply 'Own CMMC' for the Contractor

An MSP can perform many important technical functions, but CMMC readiness includes organizational decisions that an external provider cannot legitimately make on the contractor's behalf. The contractor determines its contracts, business roles, authorized users, information flows, acceptable risk decisions, internal policies, and how it fulfills responsibilities that remain with the organization.

NorthStar can configure MFA, patch systems, manage endpoints, maintain firewalls, and produce evidence for assigned services. It cannot decide without Harbor Point whether Daniel should be authorized for a sensitive project, whether a new subcontractor should receive CUI, or whether a business process should be redesigned to change the assessment scope.

This is why the responsibility matrix matters. It separates performer from owner and identifies shared functions. Outsourcing operations can improve security, but outsourcing does not erase organizational accountability.

The practical benefit is clarity during both operations and assessment. Harbor Point knows what it must decide and demonstrate. NorthStar knows what it must operate

and evidence. Neither party discovers during an incident that an important responsibility was assumed to belong to the other.

22.106 Why an Implementation Provider Is Not Automatically the Long-Term MSP

Technical implementation and ongoing operation require overlapping but different capabilities. An implementation specialist may be excellent at designing and migrating a GCC High tenant. The long-term MSP must handle user onboarding, failed devices, service changes, security alerts, patch exceptions, guest reviews, and support calls every week after the project ends.

If Harbor Point assumes the implementation provider will maintain everything indefinitely without a defined service agreement, responsibilities can fall into a gap. Conversely, if NorthStar inherits an environment without participating in handoff, its technicians may not understand the design well enough to support it safely.

This is why the three-phase implementation model ends with validation, knowledge transfer, and operational acceptance. The people who will maintain the system demonstrate that they can operate it. Documentation, credentials, diagrams, escalation paths, and known exceptions are transferred deliberately.

The why behind handoff is continuity. A secure environment that only the departing consultant understands is not operationally sustainable.

22.107 Why Operational Acceptance Testing Is Necessary

A project can pass technical tests while still failing operationally. The implementation engineer may know exactly where every setting is located, but the help desk may not know how to enroll a replacement laptop or recover a user's MFA registration. The environment works only as long as the specialist remains available.

Operational Acceptance Testing changes the question from 'Did the consultant configure it?' to 'Can the continuing organization operate it?' Harbor Point and NorthStar perform real tasks: create a user, assign approved access, enroll a device, verify protection, find logs, disable the user, retrieve evidence, and troubleshoot a controlled failure.

Failures during this test are valuable because they expose missing documentation, unclear responsibilities, inaccessible consoles, insufficient permissions, and training gaps before those weaknesses become production incidents.

Evidence from the acceptance process can include test scripts, results, corrected procedures, handoff records, and sign-off. The why is organizational independence: the operating team must be able to maintain the environment after the project team leaves.

22.108 Why Continuous Readiness Begins in the Technology Stack

CMMC readiness cannot be sustained by a one-time cleanup because technology changes continuously. Devices are added, users leave, vulnerabilities appear, cloud services change, integrations expire, and security agents fail. A control that worked on assessment day can degrade the next week.

The technology stack therefore needs mechanisms that reveal drift. Reconciliation identifies missing coverage. monitoring identifies silent log sources. patch and vulnerability systems expose aging exceptions. identity reviews reveal privilege accumulation. backup tests expose recovery problems. tickets and documentation connect changes with their purpose.

This is the bridge to Chapter 23. Continuous readiness is not an additional product installed after certification. It is the operating discipline that keeps the architecture, technology, documentation, responsibilities, and evidence aligned over time.

The Random Tuesday Test expresses this idea in practical terms. If Harbor Point can explain and demonstrate the current state without an assessment-preparation project, the security program is functioning as an everyday operating system rather than an occasional compliance exercise.

22.109 The Beginner's Full Walkthrough: Why Every Layer Exists

Priya joins Harbor Point and needs access to an engineering project. Harbor Point first authorizes the business role because technology should enforce business decisions rather than invent them. An individual identity is created because actions need to be attributable to a person. MFA is required because a password alone can be stolen. Conditional Access checks device context because a legitimate identity should not automatically make every device acceptable.

Priya receives a managed laptop because the endpoint is part of the security boundary. Device management applies the approved configuration. Encryption protects stored information if the device is lost. EDR provides behavioral security visibility. RMM allows NorthStar to maintain the computer at scale. Vulnerability management identifies weaknesses. Patch management applies and verifies updates.

Inventory establishes that the device exists and should receive all of those protections.

When Priya accesses cloud resources, Microsoft 365 Government provides the approved collaboration environment selected for Harbor Point's requirements. Network controls limit unnecessary paths. Logging records important activity. The SIEM brings relevant events together. Beacon monitors and investigates. Ticketing records authorized changes and support actions. Documentation explains the architecture. Backup and recovery address loss and disruption.

No single layer makes the environment secure. Each layer exists because another layer cannot answer every security question. Identity cannot patch the laptop. EDR cannot authorize Priya's business role. RMM cannot determine the contractual handling requirement for CUI. The SIEM cannot restore deleted data. Backup cannot prevent an unauthorized login. The strength comes from the layers working together with clear responsibility.

That is the central answer to the beginner's why question: the stack is layered because security problems are different. Prevention, authentication, authorization, visibility, management, detection, response, recovery, documentation, and evidence are distinct needs. A mature architecture connects them rather than expecting one product to solve all of them.

22.110 Final Why-and-How Perspective

The deepest lesson of Chapter 22 is that every technology decision should be traceable to a problem the organization is trying to solve. If the team cannot explain why a tool exists, what risk or operational need it addresses, who depends on it, and what would happen if it failed, the tool is not yet fully integrated into the security program.

The same standard applies to procedures. The reader should understand why MFA is required before memorizing how to enroll a user, why reconciliation matters before running a comparison report, why restore testing matters before scheduling a recovery exercise, and why government-cloud separation matters before changing an API endpoint.

Once the why is understood, the how becomes meaningful. Implementation establishes the technology. Operation keeps it functioning. Monitoring reveals failure. Troubleshooting identifies cause. Correction restores the intended state. Verification proves the correction. Evidence records the outcome. Maintenance keeps the cycle working as the environment changes.

A CMMC-ready MSP technology stack is therefore not a collection of products and not a collection of checklists. It is a reasoned operating architecture in which every major component has a security purpose, an owner, a method of operation, a method of failure detection, a recovery path, and evidence. That is the level of understanding a beginner needs before the book moves into maintaining certification and continuous readiness.

Publication Verification Note

Microsoft Government cloud details in this chapter were rechecked against current Microsoft Learn documentation during this revision. Microsoft currently describes Office 365 Government customer-content segregation and U.S. storage commitments; describes GCC High for eligible organizations including contractors holding or processing DoD CUI or subject to ITAR; documents graph.microsoft.us for GCC High while GCC continues to use worldwide Microsoft Graph endpoints; and states that devices moving from commercial Intune to the government cloud must unenroll and re-enroll because there is no built-in migration path. These service details are time-sensitive and should be revalidated during final whole-book production and future editions.

Chapter 23
Maintaining Certification and Continuous Readiness

CMMC for MSPs: From Readiness to Certification
Authored by Dr. Charles Edwards

23.1 Why Continuous Readiness Exists

An assessment is an observation of a living security program at a particular point in time. It can establish that evidence, configurations, procedures, interviews, and demonstrations support the required security outcomes at that time. It cannot freeze the organization in that condition. The next morning an employee can leave, a new laptop can arrive, a cloud service can change, an endpoint agent can stop reporting, a critical vulnerability can be published, or an administrator can modify a firewall rule. Continuous readiness exists because the environment continues moving after the assessor stops observing it.

The easiest mistake is to treat certification or assessment status as a finished construction project. That mindset creates a predictable cycle: intense preparation before an assessment, temporary cleanup, a successful assessment, and then gradual deterioration until the next deadline creates another emergency. A stronger program treats the assessed condition as the beginning of an operating baseline. Harbor Point should know what was true when it demonstrated its controls and should have mechanisms for recognizing when important facts change.

The current regulatory framework reinforces this operating concept. The current DFARS clause defines a current CMMC status in part by the age of the status and the absence of changes in compliance, and it requires annual affirmation of continuous compliance for covered CMMC UIDs. As of September 2026, DoD's official CMMC page states that implementation is paused in Phase I, with Phase I self-assessment requirements remaining in place. These current implementation details can change, but the operating lesson is durable: the organization must maintain the security condition rather than merely remember that it once demonstrated it.

23.2 What Exactly Are We Maintaining?

Continuous readiness is not the maintenance of a certificate as an isolated document. It is the maintenance of the environment and the organizational system that gave the assessment result meaning. That system includes people, identities, endpoints, networks, cloud services, applications, external providers, configurations, procedures, documentation, responsibilities, evidence, and management decisions.

Harbor Point's System Security Plan may describe how access control, monitoring, incident response, configuration management, and other requirements are implemented. NorthStar may operate many of the technical mechanisms. Beacon may monitor assigned telemetry. Microsoft may operate cloud infrastructure. If any of those underlying facts changes while the SSP and responsibility matrix remain

frozen, the paperwork can become a historical description rather than a description of the current system.

Continuous readiness therefore means maintaining alignment. The documented architecture should align with the live architecture. The asset inventory should align with the actual population. The responsibility matrix should align with the services people actually perform. The evidence should align with current operation. The security configuration should align with the approved baseline. When those relationships drift apart, readiness deteriorates even if every document still looks polished.

23.3 Why Readiness Decays

Readiness decays because organizations are designed to change. Growth creates users and devices. Projects create new data flows. Technical teams install applications. Vendors modify services. Employees change roles. Emergency troubleshooting creates temporary configurations. Mergers, new offices, subcontractors, remote work, and customer requirements reshape the boundary. None of these events is inherently a compliance failure; the failure occurs when the security program does not absorb the change.

Some decay is visible. A vulnerability report shows an aging critical finding. Other decay is silent. An EDR agent stops communicating, but the dashboard still looks mostly green. A backup system protects every system it knows about, but a new engineering server was never enrolled. A guest account remains after a project closes. An implementation consultant retains an administrative role because nobody reviewed temporary migration privileges.

The purpose of continuous readiness is to convert silent decay into visible exceptions. Inventory reconciliation, source-health monitoring, access reviews, configuration comparisons, vulnerability aging, backup reconciliation, change records, and documentation reviews all serve the same deeper purpose: they reveal where reality has moved away from the intended state.

23.4 Who Owns Continuous Readiness?

Harbor Point cannot outsource the organizational responsibility for knowing what it is protecting and how its contractual obligations apply. NorthStar can perform substantial technical work, Beacon can monitor security events, and cloud providers can operate major portions of infrastructure, but Harbor Point still decides who is authorized, which business processes handle protected information, which systems are used for contract performance, and which providers are permitted to participate.

NorthStar's responsibility is operational where the service agreement and responsibility model assign it. If NorthStar manages endpoints, it should know how endpoints enter management, how missing agents are detected, how patch failures are handled, how administrative access is controlled, and how evidence is produced. Beacon's responsibility is different: if it provides monitoring and investigation, its procedures should define source onboarding, alert handling, escalation, evidence, and loss-of-visibility response.

The dangerous situation is not shared responsibility. Shared responsibility is normal. The dangerous situation is ambiguous responsibility. If Harbor Point assumes Beacon watches backup failures, Beacon assumes NorthStar does, and NorthStar assumes Harbor Point does, a real control can fail while every organization believes another party owns it. Continuous readiness therefore requires named performers, approvers, monitors, escalation paths, evidence owners, and verification responsibilities.

23.5 What Should Happen the Day After an Assessment?

The day after an assessment should look remarkably ordinary. Administrators should not remove the configurations that were demonstrated, technicians should not stop collecting evidence, and managers should not place the SSP in a folder until the next assessment. Instead, the organization should transition from assessment support back into normal operations without losing the operating discipline that made the assessment possible.

Harbor Point should preserve the final assessed architecture, known exceptions, responsibility assignments, evidence locations, open remediation, and lessons learned as a baseline. NorthStar should ensure that temporary assessment accounts or special access used only for demonstrations are removed if no longer required. Beacon should return any temporary reporting arrangements to the normal monitored process without losing relevant records.

A useful post-assessment question is simple: which activities occurred only because an assessor was present? If technicians manually assembled reports that cannot be reproduced next month, if screenshots were staged because ordinary records were unavailable, or if dormant accounts were cleaned only for assessment week, those observations identify continuous-readiness improvements.

23.6 Why Configuration Drift Is Inevitable

Configuration drift is the difference that develops between the approved or expected configuration and the configuration that actually exists. It is inevitable because administrators make legitimate changes, software updates modify settings,

troubleshooting creates exceptions, new features appear, and emergency work sometimes bypasses the normal sequence.

Drift becomes a security problem when the organization cannot distinguish intentional change from accidental or unauthorized change. A firewall rule added through an approved ticket is different from an unexplained rule. A Conditional Access exclusion approved for a two-day migration is different from the same exclusion remaining six months later. Continuous readiness requires both a baseline and a way to recognize meaningful differences from it.

NorthStar can use configuration-management tools, platform audit logs, scripted comparisons, policy reports, and periodic reviews, but technology alone does not decide whether a difference is legitimate. The difference must be connected to authorization and business purpose. That is why change control and configuration monitoring belong together.

23.7 Practical Failure: The Temporary MFA Exception That Became Permanent

During a weekend migration, Harbor Point creates a temporary MFA exclusion for a service-related identity because an old integration cannot complete the new authentication flow. The implementation team documents that the exclusion should exist for forty-eight hours. The migration succeeds, everyone is exhausted, and Monday's operational workload begins. Nobody removes the exclusion.

Three months later, NorthStar's access review identifies the account in the exclusion group. The important control is not merely discovering that an exception exists. The team traces the original ticket, identifies the owner, confirms that the old integration was retired, removes the exclusion, tests the replacement process, and verifies that the identity can no longer use the bypass.

The root-cause improvement is to make temporary access technically and procedurally temporary. The organization may use expiration-capable mechanisms where available, scheduled review, ticket due dates, exception registers, or monitoring that identifies aged exclusions. Evidence includes the original approval, the review, the corrective change, and the verification. The lesson is that a valid exception can become an invalid weakness simply through the passage of time.

23.8 Why Personnel Changes Are Security Events

Employees join, leave, change departments, become managers, move to new projects, and receive temporary responsibilities. Every one of those events can change what

the person should be allowed to access. Continuous readiness therefore treats personnel changes as security-relevant lifecycle events rather than purely Human Resources events.

When Priya moves from one engineering project to another, adding the new group is only half the job. Harbor Point should also ask whether old project access remains necessary. Without removal, access accumulates over a career. The employee eventually possesses a historical collection of permissions that no current job requires.

Termination is even more demanding. The organization may need to disable the central identity, revoke sessions, recover devices, remove privileged roles, address VPN and remote access, remove direct SaaS accounts, revoke customer-specific portals, rotate shared secrets if they were known, and review service or API credentials associated with the individual. For an MSP technician, the population can span many customer environments.

Evidence should show the authorized event, actions taken, timing, and verification. The purpose is not merely to prove that an account was disabled. It is to demonstrate that the person's authority across the relevant environment was brought into alignment with the new business reality.

23.9 Practical Walkthrough: Robert Leaves NorthStar

Robert is a senior NorthStar technician with access to the RMM platform, PSA, documentation system, password vault, backup consoles, vulnerability platform, and several customer-specific firewall accounts. He resigns on Friday. Disabling Robert's NorthStar Microsoft account is necessary, but it is not sufficient because not every system derives authorization from that identity.

NorthStar's offboarding workflow begins with an access inventory tied to Robert's role. Central identities are disabled, active sessions are revoked where appropriate, privileged roles are removed, vault access is terminated, RMM and PSA permissions are removed, and customer-specific accounts are addressed. API tokens or credentials uniquely associated with Robert are reviewed. Harbor Point receives notification if the service agreement or customer access process requires it.

Verification is independent of the checklist. An administrator searches the major platforms for Robert's identity and checks customer-specific access. If an overlooked firewall account is discovered Monday, NorthStar removes it, reviews recent activity, and asks why the account was absent from the access inventory. The corrective action

improves the offboarding model rather than merely blaming the person who ran the checklist.

23.10 Why Every New Asset Can Change Readiness

A new asset is not simply a procurement event. It can create a new place where FCI or CUI is processed, stored, or transmitted, a new attack surface, a new administrative path, and a new evidence obligation. The organization must therefore decide what the asset is, what information it will handle, which security controls apply, and whether its introduction changes scope or documentation.

Harbor Point's provisioning workflow should connect asset creation with inventory, identity or device management, encryption, endpoint security, RMM, vulnerability management, patching, backup where required, logging, approved software, network placement, and documentation. The exact controls depend on the asset, but the workflow should prevent the asset from becoming operational before required protections are established.

The deeper control is reconciliation after provisioning. If the new laptop appears in inventory but not EDR, the discrepancy becomes an exception. If a new server appears in RMM but not backup, the omission is detected. Continuous readiness is strengthened when the environment can identify incomplete onboarding without waiting for an assessor to sample the missing system.

23.11 Practical Failure: The New Engineering Server

Harbor Point's engineering group needs a server urgently for a new project. An administrator builds ENG-SRV-07, joins it to the environment, installs the application, and gives the project team access. The server appears in RMM because the standard build includes the RMM agent. The engineer assumes the remaining protections are automatic.

At the monthly reconciliation, ENG-SRV-07 appears in inventory and RMM but is missing from the vulnerability platform and backup service. EDR is present but reporting an incorrect policy. The system has already begun storing project information. This is not one failure; it is evidence that the provisioning workflow allowed a production system to bypass several gates.

NorthStar and Harbor Point first protect the live system: correct EDR policy, enroll vulnerability assessment, establish backup according to the recovery design, and verify each service. They then examine the provisioning process. The lasting fix may be a build checklist, automation, approval gate, reconciliation rule, or combination of

controls. Evidence includes the detected discrepancies, remediation tickets, final health verification, and updated process.

23.12 Why New Software, SaaS, and AI Can Change Scope and Risk

Modern technology can enter an organization without a traditional installation project. An employee can authorize a SaaS application, add a browser extension, create an AI account, connect an OAuth application, or subscribe to a cloud service with a credit card. If protected information enters that service, the organization's information flow and provider relationships may change immediately.

Continuous readiness therefore needs a technology-intake process. Before Harbor Point approves a service for CUI or other protected information, it should understand the function, information involved, provider, authentication, administrative controls, data flow, retention, integrations, logging, contractual suitability, and exit strategy. NorthStar can provide technical analysis, but Harbor Point owns the business decision about authorized use.

The why is not to slow innovation. The purpose is to prevent architecture from being created accidentally by individual user choices. A ten-dollar SaaS subscription can create a new external information system just as surely as a six-month infrastructure project.

23.13 Why New CUI Flows Demand Immediate Attention

CUI scope follows information and the systems and services that process, store, or transmit it. When Harbor Point changes where CUI goes, it may change the systems, people, providers, network paths, and documentation relevant to its security program. This is why a new information flow deserves review before it becomes routine.

Suppose Harbor Point begins sending engineering data to a new subcontractor. The business team may view the change as a purchasing decision. Security must ask how the information will be transferred, which systems will store it, what contractual requirements flow down, how recipient authorization is established, what service providers participate, and whether Harbor Point's diagrams and SSP still describe the actual flow.

The control should be event-driven. The organization should not wait for a quarterly meeting to discover that CUI began flowing to a new environment three months earlier. Procurement, contracting, project management, and IT need a trigger that brings the proposed flow into security review.

23.14 Why Asset Reconciliation Must Continue Forever

An inventory can be accurate on assessment day and wrong a week later. Devices are replaced, virtual machines are cloned, systems are rebuilt, laptops remain offline, records become duplicated, and retired devices remain in management consoles. Continuous reconciliation is therefore a permanent operating function.

Harbor Point and NorthStar compare the authoritative population with systems that provide protection or management. The useful output is not a single percentage. It is a list of unexplained differences. A device missing from EDR requires investigation. A device present in EDR but absent from inventory may be a stale record, an unauthorized asset, or an asset whose inventory record was lost.

Reconciliation should also occur after major events such as migrations or RMM replacement. The question is always whether the expected population and the observed population match closely enough that every difference can be explained. That discipline detects silent failure that product dashboards cannot detect by themselves.

23.15 Why Security Tool Health Must Be Monitored

Security tools can fail silently. Agents stop communicating, connectors expire, licenses lapse, certificates expire, APIs change, storage fills, policies fail to deploy, and service accounts lose permission. The organization can believe a control is operating because the product still exists while the protective function has degraded.

NorthStar should define health for each important platform. EDR health may include agent presence, recent communication, correct policy, and sensor state. SIEM health includes expected source activity. Vulnerability-management health includes asset coverage and scan success. Backup health includes protected population, job success, and recoverability. RMM health includes agent communication and management capability.

The reason to define health is operational ownership. A red indicator has little value if nobody receives it, knows what it means, or has authority to fix it. Continuous readiness connects health conditions to alerts, tickets, owners, escalation, correction, and verification.

23.16 Practical Failure: Beacon Loses a Log Source

Beacon normally receives firewall events from Harbor Point. The connector depends on a certificate that expires. At 2:00 a.m. the firewall continues protecting the

network, but the event stream stops reaching the SIEM. No attack alert announces the loss because the problem is the absence of data.

A source-health rule notices that an expected high-volume source has become stale and opens an escalation. Beacon confirms the gap and notifies NorthStar. NorthStar traces the collection path, identifies the expired certificate, replaces it through the approved process, and verifies that new events arrive with correct timestamps and fields.

The incident is not closed there. The team determines why the certificate expiration was not tracked, adds the credential to lifecycle management, and reviews whether the visibility gap requires additional investigation. The evidence demonstrates detection of control degradation, restoration, verification, and process improvement.

23.17 Why Vulnerability Management Never Ends

An assessment cannot certify that no new vulnerabilities will be discovered. Software changes and researchers discover weaknesses continuously. A system that was fully patched yesterday can become vulnerable today when a new issue is disclosed. Continuous readiness therefore requires a recurring vulnerability-management process.

The process begins with awareness and coverage. Harbor Point and NorthStar need to know which assets and applications are relevant and whether the vulnerability process can assess them. Findings are then interpreted in context. Severity matters, but so do exploitability, exposure, business importance, CUI relevance, active exploitation, and available mitigations.

Ownership follows prioritization. NorthStar may patch a workstation, an application vendor may need to provide an update, Harbor Point may need to approve downtime, or a network team may implement temporary restrictions. The program tracks the finding until the intended risk treatment is verified.

Evidence should tell the story from discovery through closure. A scanner report alone proves discovery. Tickets, approvals, remediation records, exceptions, rescans, and validation demonstrate the operating lifecycle.

23.18 What Happens When a Critical Vulnerability Appears Tuesday Morning?

At 9:10 a.m. NorthStar receives credible notice of a critical vulnerability affecting a product used by several customers. The first task is not mass patching. The first task

is determining whether Harbor Point actually uses the affected versions and where they exist. Asset and software inventory become essential.

If Harbor Point is affected, the team evaluates exposure and available vendor guidance. Beacon may increase monitoring for relevant indicators. NorthStar may apply a vendor patch, disable a vulnerable feature, restrict network access, or use another temporary mitigation. Harbor Point may need to approve downtime for an engineering service.

After remediation, the team verifies the actual condition. A patch installation record is not enough if the vulnerable version remains active. The vulnerability platform, configuration check, version query, or other appropriate method confirms the outcome. Any temporary mitigation remains tracked until permanent resolution. This is continuous readiness in action: new risk enters the environment, becomes owned work, and leaves behind evidence.

23.19 Why Automatic Updates Do Not Replace Patch Management

Automatic updates solve part of the deployment problem, but they do not solve exception management. Devices can be offline, updates can fail, reboots can remain pending, production systems can require maintenance windows, firmware may use different mechanisms, and applications can have independent update channels.

A patch-management program therefore focuses on the tail of the distribution. Ninety-eight successful devices may require little attention; the two failures may contain the greatest remaining risk. NorthStar identifies them, determines why they failed, corrects the condition, and verifies the outcome.

Where an update cannot immediately be applied, the exception should have an owner, reason, risk understanding, temporary protections where appropriate, and review point. The purpose is to keep inability to patch from becoming invisibility.

23.20 Why Backup Readiness Must Be Proven Through Recovery

Backup is a promise about the future: if something is lost, the organization expects to recover it. A successful backup job is evidence that data was copied according to a process; it is not complete proof that the business service can be restored.

Harbor Point therefore performs restore tests at a depth appropriate to the service. A file-share test may restore selected files and permissions. An engineering application may require a server, database, license service, identity dependency, and configuration. The test should prove the recovery outcome the business actually needs.

Failures are valuable. If the restoration fails because a database credential was not documented, the test has found a readiness weakness without a real disaster. NorthStar corrects the recovery documentation, repeats the test, and records the verified result. Continuous readiness uses controlled testing to discover failure before the emergency.

23.21 Practical Failure: The Restore That Almost Worked

Harbor Point schedules a recovery test for an engineering application. NorthStar restores the application server successfully and confirms that the operating system starts. The team initially considers the test successful.

Daniel opens the application and receives a licensing error. Investigation reveals that the license service is a separate virtual machine that was not included in the recovery runbook. The application server is technically restored, but the business capability is unavailable.

The recovery design is updated to include dependencies, restoration order, credentials, validation steps, and responsible parties. A second test restores the complete service. The evidence now demonstrates something much stronger than a green backup dashboard: Harbor Point can recover the engineering capability it depends upon.

23.22 Why Microsoft 365 Government Requires Continuous Administration

Microsoft operates the cloud service, but Harbor Point operates its use of the service. Microsoft does not know that Priya changed projects, that a guest relationship ended, that a particular SharePoint site contains CUI, or that a temporary administrative role is no longer necessary. Those are customer-side decisions.

Continuous administration includes identity lifecycle, MFA, Conditional Access, privileged roles, guest access, licensing, Exchange configuration, Teams and SharePoint governance, OneDrive lifecycle, Intune device management, Defender or other endpoint security, application registrations, integrations, and service changes. NorthStar may perform many of these tasks, but Harbor Point supplies business authorization and governance.

Cloud services also evolve. Features are introduced, deprecated, or changed. APIs and endpoints can change. The operating team needs a service-change process that identifies relevant changes, evaluates impact, tests where necessary, updates

integrations or procedures, and records significant architecture changes. Cloud does not remove maintenance; it changes the form of maintenance.

23.23 Why Privileged Access Must Be Re-Justified

Privilege is often granted because somebody needs to complete a task. The task ends, but the privilege can remain. Over time, administrators accumulate rights from old projects, migrations, emergencies, and temporary responsibilities. Continuous readiness therefore treats privilege as something that must remain justified, not something granted permanently by default.

Harbor Point reviews its privileged roles and NorthStar reviews technician access. The review asks whether each person still requires each role, whether direct assignments can be reduced, whether temporary elevation is more appropriate, and whether inactive or emergency accounts are correctly controlled.

The evidence is not merely a list of administrators. It includes the review decision and resulting changes. If Maria no longer supports Harbor Point, removal of her customer access should be visible. If an implementation account remains because a vendor still supports the tenant, that continued need should be documented and periodically reconsidered.

23.24 Why Evidence Becomes Stale

Evidence has a time dimension. A screenshot showing MFA policy from eight months ago proves that a configuration appeared a certain way eight months ago. It does not by itself prove that the configuration remains unchanged today. The more dynamic the control, the more important current operational evidence becomes.

This does not mean Harbor Point should take screenshots every day. It means the evidence strategy should use authoritative records generated by normal operation where possible: audit logs, configuration exports, ticket histories, access reviews, inventory reconciliations, vulnerability records, patch reports, backup tests, and incident records.

Historical evidence remains valuable because it demonstrates operation over time. Current evidence demonstrates present condition. A mature evidence library can show both. The organization should understand which question each artifact answers instead of treating all evidence as interchangeable.

23.25 How Should Evidence Be Maintained Without Creating a Screenshot Factory?

Evidence should be designed around claims. If Harbor Point claims that terminated users lose access, the useful evidence is the offboarding workflow plus sampled records showing that the workflow occurred. If it claims that endpoints are protected, useful evidence includes the authoritative asset population, security-platform coverage, reconciliation, and exception resolution.

NorthStar should identify which records already exist in operational systems before inventing manual evidence tasks. The PSA records work. Identity logs record administrative actions. EDR records endpoint state. Vulnerability systems record findings and verification. Backup systems record jobs and tests. The evidence process organizes and preserves the right records rather than duplicating every console into screenshots.

Where retention or licensing can remove historical records, Harbor Point and NorthStar should understand that limitation and design preservation appropriately. Evidence ownership should identify who can retrieve the record, where it lives, and what happens if a provider or platform is replaced.

23.26 Why the SSP Must Change When Reality Changes

The SSP is valuable because it describes the system and how security requirements are implemented. If the live environment changes but the SSP does not, the document becomes less trustworthy. Continuous readiness therefore treats the SSP as controlled operational documentation rather than a one-time assessment deliverable.

Not every help-desk ticket requires an SSP revision. The organization should identify changes significant enough to affect scope, architecture, control implementation, external-provider relationships, CUI flows, or the description of how a requirement is satisfied. A new laptop normally updates inventory without rewriting the architecture narrative. A new cloud provider handling CUI may require substantial documentation review.

Event-driven review is supplemented by periodic validation. Harbor Point can compare the SSP, diagrams, responsibility matrix, and live systems. Discrepancies become corrections or evidence of a deeper change-management problem.

23.27 When Should the Responsibility Matrix Change?

The responsibility matrix should change when responsibility changes. If NorthStar begins managing backups that Harbor Point previously managed internally, the

documentation should reflect the new performer, approvals, monitoring, escalation, evidence, and verification. If Beacon is replaced, monitoring responsibilities and evidence locations change.

The matrix is not merely an assessment aid. It is an operating map. During an incident, the team should be able to determine who acts. During onboarding, it should be clear who configures a device. During evidence collection, it should be clear who produces the relevant records.

A quarterly or other periodic review can catch drift, but major provider or service changes should trigger immediate review. Waiting for the next scheduled meeting can leave a real operational gap.

23.28 What Happens When the MSP Replaces Its Own RMM?

NorthStar decides to replace its RMM platform. From NorthStar's perspective, this is an internal technology modernization. From Harbor Point's perspective, it changes a security-relevant administrative path into its environment. The migration therefore deserves controlled planning.

NorthStar inventories managed Harbor Point systems, defines old and new agent populations, reviews technician roles, automation, scripts, integrations, logging, customer separation, and API access. During migration, both old and new platforms may coexist. That temporary state can create duplicate agents, inconsistent policies, or expanded administrative authority.

The migration is not complete when the new console shows devices. NorthStar reconciles the expected Harbor Point population, verifies remote management and monitoring, removes old agents, revokes obsolete API tokens, disables old technician access, preserves required historical records, updates documentation, and confirms that Harbor Point's evidence processes still work.

This scenario demonstrates why an MSP's internal change can affect a customer's continuous readiness. The service provider's technology is part of the operating security system.

23.29 What Happens When an External Provider Changes?

Replacing a SOC, backup provider, cloud application, or MSP creates both an onboarding and an offboarding problem. The new provider needs authorized access and context; the old provider must lose access and return or appropriately handle information, credentials, integrations, and records according to the applicable agreement and requirements.

Harbor Point should identify what the outgoing provider can access, what accounts and API connections exist, where evidence is stored, which logs need preservation, and what dependencies must be migrated. The incoming provider should be validated before the old capability disappears where continuity is required.

The responsibility matrix, SSP, diagrams, escalation procedures, and evidence locations may all change. Provider transition is therefore a security architecture event, not merely a purchasing event.

23.30 Why Incidents Must Change the Program

An incident reveals how the security system behaves under stress. If Harbor Point contains an incident and then restores the environment exactly to the previous state without asking what allowed the event or what made response difficult, it loses much of the value of the investigation.

Lessons learned can affect configuration, monitoring, training, procedures, architecture, provider responsibilities, evidence, or recovery. A phishing incident may reveal that a legacy protocol remains enabled. An endpoint incident may reveal that isolation authority is unclear. A delayed investigation may reveal that a needed log source is not retained long enough.

Not every incident requires a major redesign. The purpose is disciplined learning. The team identifies material lessons, assigns improvements, tracks them, verifies implementation, and updates relevant documentation. Continuous readiness improves because incidents become inputs to the program rather than isolated emergencies.

23.31 Why Exceptions Need a Lifecycle

Exceptions exist because business and technology are imperfect. The security program becomes weak when exceptions are invisible or immortal. A temporary firewall rule, unpatched legacy server, guest account, MFA exclusion, or administrative privilege should not survive simply because nobody remembers why it exists.

A controlled exception records the intended requirement, the actual deviation, business reason, owner, risk, temporary protections, approval, target resolution, and review date. The owner must be capable of driving the issue to a decision rather than merely receiving email reminders.

At review, the exception is closed, renewed with current justification, modified, or escalated. Evidence shows that the organization knows about the deviation and is

actively governing it. This is very different from discovering the condition for the first time during an assessment.

23.32 What Should Happen Every Day?

Daily readiness is primarily exception-driven. NorthStar and Beacon should not manually inspect every healthy system each morning. Automated platforms should surface conditions requiring human attention: critical alerts, failed backups, missing agents, stale log sources, failed patches, account problems, suspicious activity, and high-impact service incidents.

Technicians and analysts investigate those exceptions through controlled workflows. Harbor Point provides business decisions when required. The important daily outcome is that serious failures do not remain invisible and that unresolved items have owners.

Daily operation also creates evidence naturally. Alerts, tickets, administrative logs, backup records, and remediation actions form an operational history. The program becomes stronger when those records are consistent enough that assessment evidence can later be drawn from normal work.

23.33 What Should Happen Every Week?

Weekly review looks beyond individual alerts to unresolved operational patterns. NorthStar can examine failed patch populations, stale agents, vulnerability queues, backup exceptions, new assets, unresolved access requests, and significant changes. Beacon can review notable detections, source-health issues, and recurring alert patterns.

The weekly rhythm is useful because some issues are not emergencies but should not wait a month. A laptop that has been offline for several days may be legitimate travel or may represent a device falling out of management. A vulnerability repeatedly deferred by a project team may require management attention.

The objective is to keep the exception backlog from becoming a hidden second environment in which known problems accumulate without resolution.

23.34 What Should Happen Every Month?

Monthly review provides a broader operational picture. Harbor Point and NorthStar can reconcile major asset populations, review vulnerability aging, patch exceptions, endpoint coverage, backup coverage, privileged changes, guest accounts, service health, major change tickets, and documentation impacts.

Management should see both performance and exceptions. A 99 percent EDR coverage metric should be accompanied by the identity and disposition of the missing one percent. A high patch-success rate should not conceal an unpatched Internet-facing server. Metrics become useful when they lead to questions about residual conditions.

Monthly review also provides a natural point to verify that responsibilities remain functional. Are escalations reaching the right people? Are evidence records retrievable? Are customer contacts current? Are provider dependencies healthy?

23.35 What Should Happen Quarterly?

Quarterly review is well suited to deeper governance activities that do not need daily execution. Harbor Point can review privileged access, guest populations, responsibility assignments, major documentation, provider relationships, exception aging, recovery-test results, and significant architecture changes.

NorthStar can perform customer security reviews that connect technical trends to business decisions. If vulnerability aging is increasing because Harbor Point cannot schedule downtime, the issue has moved beyond technician performance and requires management action. If guest access grows continuously, the business process for external collaboration may need attention.

Quarterly does not mean every control must wait three months. High-risk events remain event-driven. The periodic review exists to detect slow drift and accumulated change.

23.36 What Should Happen Annually?

Annual activities should confirm that the program still reflects the organization and its obligations. This can include policy review, broader SSP validation, responsibility review, risk and architecture review, training refresh, recovery exercises, provider review, and preparation for applicable affirmation or assessment obligations.

Current CMMC requirements make annual affirmation especially important where applicable. The affirmation should not be treated as a ceremonial click. The affirming official needs an organizational process capable of supporting the assertion of continuous compliance. The technical and governance reviews throughout the year should make that decision informed rather than speculative.

Annual review also asks whether the previous year's operating rhythm worked. Which controls repeatedly failed? Which metrics were misleading? Which evidence

was difficult to retrieve? Which provider responsibilities were unclear? The answers shape the next year's improvement priorities.

23.37 What Events Should Trigger Immediate Review?

Scheduled reviews are not enough because some changes alter risk immediately. New contracts, new CUI flows, new systems, new external providers, new locations, acquisitions, major cloud migrations, significant security incidents, MSP changes, SOC changes, privileged-access redesign, and major network architecture changes should trigger security review when they occur.

The trigger should exist in the business process that learns about the change first. Procurement can trigger provider review. Human Resources can trigger identity lifecycle. Project management can trigger new CUI-flow review. IT change management can trigger architecture documentation. Contracting can trigger CMMC and flowdown review.

This is how continuous readiness becomes organizational rather than an IT side project. Security learns about meaningful change early enough to shape it.

23.38 What Metrics Actually Tell Management Something Useful?

Metrics should help management make decisions. Counts and percentages without context can create false confidence. 'Ninety-nine percent patched' sounds excellent until management learns that the remaining one percent contains the only Internet-facing server handling an important service.

Useful measures often combine coverage, exception, age, and consequence. Examples include expected versus protected endpoints, critical vulnerabilities by age and owner, failed backup jobs plus missing backup coverage, stale log sources, privileged accounts awaiting review, open high-risk exceptions, restore-test success, and time to close significant security incidents.

The goal is not to create a giant dashboard. A small set of measures that exposes unresolved risk is more useful than dozens of green indicators. Management should be able to ask what remains outside the intended state and what decision is needed.

23.39 What Is the Difference Between a Metric and Evidence?

A metric summarizes. Evidence demonstrates. A metric may state that 99.2 percent of endpoints reported healthy EDR status this month. Evidence can show the underlying endpoint population, the missing devices, investigation tickets, and verified corrections.

Both are useful. Management needs summaries to identify trends and allocate attention. Assessors and internal reviewers may need samples and records that demonstrate how the process actually operates. Confusing the two can produce either an overwhelming evidence dump or an attractive dashboard that proves very little.

Continuous readiness connects them. Metrics identify where to investigate; operational records show what happened; evidence demonstrates the process and outcome.

23.40 What Happens When Continuous Monitoring Finds a Failure?

The response lifecycle should be predictable even when the failure is not. Detection creates a record. Ownership is assigned. The team determines scope and urgency. Containment is used if necessary. The underlying cause is investigated. Corrective action is implemented. The result is verified. Documentation and evidence are updated. Root cause and recurrence prevention are considered.

Suppose vulnerability scanning stops on twenty laptops. NorthStar first confirms whether the issue is a scanner outage, network problem, failed agent, licensing issue, or population change. It restores the capability and verifies that the laptops return to assessment. It then asks why monitoring did not identify the degradation sooner if the failure existed for days.

The purpose of the lifecycle is to avoid the common pattern in which a technician performs a plausible fix and closes the ticket without proving that the security function returned.

23.41 How Do We Prepare for the Next Assessment Without an Assessment Cleanup Project?

The best preparation for the next assessment is a year of ordinary disciplined operation. Harbor Point should not need to reconstruct who had administrator access six months ago if access reviews and logs already exist. NorthStar should not need to invent patch evidence if the patch and exception process has been operating continuously. Beacon should not need to recreate monitoring history if alert and source-health records are retained.

Before an assessment, the organization will still organize evidence, confirm scope, schedule participants, and perform readiness checks. That is normal preparation. The distinction is that preparation should assemble and validate an existing program rather than manufacture a temporary one.

The Random Tuesday Test is useful throughout the year: if an assessor unexpectedly asked a reasonable operational question today, could the team answer from current systems and records? Where the answer is no, the organization has found a continuous-readiness improvement.

23.42 One Year Later: Is Harbor Point Still Ready?

One year after its assessment, Harbor Point looks different. Daniel moved to another department. Priya received a replacement laptop. Two employees left. ENG-SRV-07 was added. A new subcontractor began receiving CUI. Microsoft changed part of a cloud service. NorthStar migrated its RMM. Beacon investigated an endpoint incident. Several critical vulnerabilities were remediated. One production patch required an exception. A recovery test failed before succeeding on the second attempt. A temporary guest account was discovered during review.

The correct question is not whether change occurred. Change is expected. The question is whether each change entered the security operating system. Daniel's old access should have been reviewed when his role changed. Priya's old laptop should have been retired and the replacement fully enrolled and reconciled. Departed employees should have lost all relevant access. ENG-SRV-07 should have entered inventory and every applicable protection. The subcontractor relationship should have triggered information-flow, contractual, and security review.

NorthStar's RMM migration should have preserved customer separation, historical evidence where required, agent coverage, scripts, integrations, and administrative accountability. Beacon's incident should have produced lessons learned. The critical vulnerabilities should have an evidence trail from discovery through verification. The patch exception should remain visible until closed. The failed recovery test should have improved the recovery plan. The guest account should have been removed and the review process strengthened.

If Harbor Point can show those histories from normal records, explain current architecture, identify open exceptions, demonstrate current control health, and produce current evidence without a frantic cleanup campaign, it has a functioning continuous-readiness program. If those answers depend on memory and emergency reconstruction, the year's changes have outrun the security program.

23.43 The Current Regulatory Context and Why the Book Must Distinguish It From the Operating Principle

As of September 2026, DoD's official CMMC information states that the program is paused in Phase I following the July 2026 suspension of the planned Phase II

requirements. The same official page states that Phase I self-assessment requirements remain in place, including annual Level 1 self-assessment and affirmation and Level 2 self-assessment every three years with annual affirmation. Current DFARS 252.204-7021 also requires covered contractors to maintain a current required CMMC status for the duration of the contract and complete annual affirmation of continuous compliance for applicable CMMC UIDs.

Those implementation details are time-sensitive and should be revalidated whenever this book is updated. A regulation can change faster than the operating principles in this chapter. The durable principle is that a contractor handling protected government information must not confuse a dated assessment record with continuing security. People, systems, information flows, providers, vulnerabilities, and configurations continue changing regardless of the assessment calendar.

For that reason, this chapter intentionally teaches continuous readiness as an operating discipline first and a regulatory obligation second. The operating discipline remains useful even when implementation phases, assessment mechanisms, or contract clauses evolve.

23.44 Closing Perspective: Readiness Is a Condition You Operate

Continuous readiness is not continuous assessment. Employees should not spend every day pretending an assessor is watching. They should spend every day operating the security program correctly. When that happens, evidence accumulates naturally, exceptions remain visible, documentation follows meaningful change, and management can understand the current state.

Harbor Point does not need a perfect environment. NorthStar will encounter failed agents and patches. Beacon will investigate false positives and real incidents. Microsoft and other vendors will change services. Employees will make mistakes. Continuous readiness is the ability to recognize those realities, assign ownership, correct material failures, verify outcomes, learn, and preserve an accurate record.

The most important test is therefore not 'Did we pass?' It is 'Does the system we demonstrated still exist and still operate the way we say it does?' That question connects the assessment, the technology stack, the MSP's daily work, the contractor's accountability, and the evidence program.

Normal operations should create security. Normal operations should create evidence. Normal operations should maintain readiness. When those three statements are true on an ordinary Tuesday, the organization is no longer preparing for CMMC as an event. It is operating a security program capable of remaining ready.

Authoritative Sources for Current CMMC Statements

Department of Defense CIO, CMMC About page, current as reviewed September 2026: https://dodcio.defense.gov/CMMC/About/

Acquisition.gov, DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025): https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements.

Acquisition.gov, DFARS 204.7502, CMMC Policy: https://www.acquisition.gov/dfars/204.7502-policy.

Regulatory and implementation details are time-sensitive. They should be rechecked against current authoritative sources during final whole-book production and before future editions are published.

Chapter 23 Expanded Teaching Laboratory: Answering the Questions Behind Continuous Readiness

The earlier sections established the framework. This expansion answers the questions a new contractor, new MSP, new technician, or new security manager is likely to ask when the phrase continuous readiness moves from policy language into daily work. The emphasis is deliberately operational. Each section explains why the activity exists, who performs it, what happens in practice, how failure is recognized, how the organization responds, what evidence remains, and how the activity connects back to the larger CMMC program.

23.45 How Does a Small Contractor Build Continuous Readiness From Nothing?

A small defense contractor does not begin by creating a security operations center, buying every security product, or hiring a full compliance department. It begins by identifying the environment it actually has. Management needs to know which contracts involve FCI or CUI, where that information enters the organization, where it is stored, who uses it, which devices and services participate, and which external providers support those systems. Without that picture, a continuous-readiness program has no defined object to maintain.

The next step is to translate the environment into ownership. Harbor Point identifies an internal accountable leader even if that person has several other responsibilities. NorthStar identifies the service manager or technical owner responsible for the customer. Beacon identifies the monitoring and escalation contacts. Each important function receives a performer and an escalation path. A small company does not need dozens of committees; it needs clarity.

Then the organization establishes a baseline. The baseline is the agreed current state: asset population, approved users, privileged identities, security platforms, network architecture, cloud environment, major policies, provider relationships, known exceptions, and evidence locations. Continuous readiness begins when the company can recognize meaningful departures from that baseline.

The final starting step is an operating rhythm. Daily attention is driven by alerts and failures. Weekly attention focuses on unresolved exceptions. Monthly attention examines coverage and trends. Quarterly attention validates privileges, responsibilities, documentation, providers, and recovery. Event-driven reviews occur whenever the business changes in ways that affect information, systems, people, or

providers. The program can become more sophisticated later, but these basic mechanisms give a small contractor a functioning security operating system.

23.46 What Does the First Monday Morning Actually Look Like?

At 8:00 Monday morning, Harbor Point does not open a CMMC checklist and begin checking 110 requirements one by one. Continuous readiness should be integrated into ordinary operations. Beacon reviews overnight security alerts and source-health conditions. NorthStar reviews high-priority tickets, failed backups, security-agent health, critical vulnerability notices, patch exceptions, and service incidents. Harbor Point's internal point of contact reviews items requiring business authorization or management decisions.

Suppose Beacon has no critical incident, but NorthStar sees three exceptions: Priya's laptop has not checked into EDR for thirty-six hours, one backup job failed, and a critical vulnerability advisory affects a product that may exist on Harbor Point's engineering network. Those three items become the morning's readiness work because they represent uncertainty about the intended security state.

NorthStar first determines whether Priya is traveling or whether the EDR agent failed. It determines whether the backup failure is transient or whether the protected system is at risk of losing recoverability. It checks software inventory to determine whether the vulnerable product is present. Each investigation creates or updates a ticket so that ownership, findings, actions, and verification are recorded.

Harbor Point becomes involved when a technical exception requires a business decision. If patching the vulnerable engineering system requires four hours of downtime, NorthStar should not silently choose the business impact. Harbor Point decides when the outage can occur after receiving the security context. The MSP supplies technical analysis; the contractor supplies business authority.

23.47 Who Looks at Which Dashboard, and Why?

A common failure in managed environments is purchasing many dashboards without deciding who is responsible for watching them. A dashboard is not a control merely because it contains green and red indicators. The organization must define which conditions matter, who receives them, how quickly they require attention, and what action follows.

Beacon may watch the SIEM and security detections because its function is continuous security monitoring. NorthStar may watch RMM health, patching, backup, endpoint coverage, vulnerability status, and service-management queues

because those are managed operational functions. Harbor Point management does not need to stare at every console. It needs meaningful reports and escalation when technical conditions require business decisions.

Responsibilities can overlap deliberately. NorthStar may also receive EDR alerts while Beacon performs deeper investigation. Harbor Point may have read access to dashboards for transparency. The important question is not who can see a dashboard but who is accountable for acting when a defined condition appears.

The team should also monitor the monitors. If Beacon's SIEM loses firewall logs, somebody must notice the absence. If NorthStar's vulnerability scanner stops reaching a network segment, somebody must recognize the coverage gap. Continuous readiness therefore includes platform-health alerts in addition to the security events those platforms detect.

23.48 Who Opens the Ticket?

The person or system that first recognizes actionable work should create the operational record unless the service model explicitly routes creation elsewhere. Automation can open tickets for failed backups, missing agents, or critical alerts. Beacon can create or escalate an incident record. A NorthStar technician can open a ticket when a discrepancy is found during review. Harbor Point can open a request when a business change requires technical action.

The ticket should not become an administrative obstacle that delays urgent response. During an active incident, containment may begin immediately under pre-authorized procedures while the record is created concurrently. The purpose is traceability, not ceremony.

A useful ticket answers enough questions that another qualified person can understand what happened. What condition was observed? Which customer and asset were involved? What was the risk or business impact? Who authorized the action when authorization was required? What did the technician do? What was the result? How was the result verified? What remains open?

Ticket ownership should also change deliberately. Beacon may identify suspicious activity and assign action to NorthStar. NorthStar may determine that Harbor Point must approve downtime. The record should make that handoff visible so that a task does not disappear between organizations.

23.49 Who Decides Whether Something Is Important?

Importance is determined by context, not by the color a vendor assigns to an alert. A critical vulnerability on an isolated test system may require a different response from a medium-severity weakness on an Internet-facing system containing sensitive information. A low-confidence EDR alert on a domain administrator's workstation may deserve more attention than a high-confidence nuisance event on a disposable kiosk.

Beacon contributes threat and detection context. NorthStar contributes technical and asset context. Harbor Point contributes business and information context. When those perspectives are combined, the team can determine urgency more intelligently.

Organizations should define escalation categories before incidents occur. A condition involving suspected CUI exposure, privileged-account compromise, ransomware, broad service outage, loss of monitoring, or significant backup failure may require immediate escalation. Routine patch exceptions or individual device-health issues may remain within normal service operations unless their context raises the risk.

The objective is consistency without rigidity. Predefined severity criteria help people act quickly, but qualified staff should be able to escalate when circumstances make an apparently ordinary event unusually consequential.

23.50 When Does the Contractor Need to Become Involved?

The MSP should handle routine technical work within its authorized service boundaries without asking the contractor to approve every normal action. Otherwise managed service becomes unmanageable. Harbor Point does not need to approve every standard endpoint signature update or every routine maintenance task that the service agreement already authorizes.

The contractor becomes necessary when the decision belongs to the business or changes accepted risk, access, scope, architecture, contractual handling, or operational impact. Granting a user access to a CUI project, accepting extended downtime, approving a security exception, onboarding a new provider, changing how CUI is exchanged, or accepting a significant residual vulnerability are examples where Harbor Point's authority matters.

NorthStar should know the boundary in advance. A responsibility matrix and service agreement can distinguish pre-authorized operational actions from customer-approved changes. Emergency procedures can define actions the MSP may take immediately to protect the environment when delay would materially increase harm.

This prevents two opposite failures. The first is an MSP that acts beyond its authority. The second is an MSP that refuses to take necessary protective action because every decision requires locating a customer executive at 2:00 a.m.

23.51 When Should the SOC Contact the MSP Directly?

Beacon should contact NorthStar directly when investigation identifies a technical action within NorthStar's assigned authority or when NorthStar possesses the operational context needed to continue the investigation. Examples include isolating an endpoint, checking an RMM record, validating a patch, reviewing a firewall configuration, collecting endpoint information, or confirming whether an administrative action was legitimate.

The escalation should include enough context to avoid a blind instruction. Beacon should identify the affected asset or identity, observed behavior, relevant timestamps, severity, requested action, and whether immediate containment is recommended. NorthStar should acknowledge receipt and record its response.

Harbor Point should be included according to the incident plan and severity thresholds. A minor false positive does not necessarily require an executive call. Suspected compromise involving CUI, privileged accounts, material service disruption, or reporting implications should follow the defined management and incident-response escalation path.

The relationship works best when Beacon, NorthStar, and Harbor Point practice it before a crisis. A tabletop exercise can reveal that phone numbers are obsolete, after-hours contacts are unclear, or the MSP lacks authority to perform the action the SOC assumes it can perform.

23.52 What Happens After Hours?

Cybersecurity events do not respect business hours. The after-hours model therefore needs to answer who is watching, who can be reached, which actions are pre-authorized, and when management must be awakened. These decisions should be made calmly before an emergency.

Beacon may provide twenty-four-hour monitoring. NorthStar may provide an on-call technician. Harbor Point may identify a primary and secondary management contact. The incident plan defines thresholds. A routine blocked malware event may be documented for morning review. Evidence of active ransomware or privileged compromise may trigger immediate containment and management escalation.

After-hours authority is especially important. If a compromised workstation is actively communicating with an attacker, waiting three hours for a manager to approve isolation may be unreasonable. Harbor Point can pre-authorize Beacon or NorthStar to isolate endpoints under defined conditions while requiring immediate notification and documentation.

Pre-authorization does not remove accountability. The next business day the team reviews what happened, whether the action was appropriate, what business impact occurred, and whether procedures need adjustment.

23.53 Who Has Authority to Isolate a Computer?

Endpoint isolation can interrupt an employee's work and, in some cases, disrupt a critical business process. It can also stop an attacker from continuing lateral movement or data access. The organization must balance those consequences before an incident.

Harbor Point should define classes of systems and isolation authority. Ordinary user workstations may be pre-authorized for immediate isolation when Beacon confirms specified high-confidence conditions. Critical production systems may require additional coordination unless evidence indicates imminent harm. NorthStar and Beacon need to know which category an asset belongs to.

The procedure should also address verification. After isolation, the team confirms that the endpoint is actually contained, preserves relevant evidence, investigates associated identities and systems, and determines the recovery path. Isolation is a containment action, not the end of incident response.

The ticket or incident record captures who initiated isolation, under which authority, why, when, what happened afterward, and when the system was safely returned to service.

23.54 Who Can Disable an Account?

Account disabling can be both a routine lifecycle action and an emergency containment action. Human Resources or management may authorize termination-related disablement. During an incident, Beacon may recommend immediate action because an identity appears compromised. NorthStar may possess the technical ability to perform the disablement.

The operating model should distinguish recommendation, authorization, and execution. For ordinary personnel actions, Harbor Point authorizes and NorthStar executes if assigned. For a high-confidence active compromise, Harbor Point may

pre-authorize NorthStar or Beacon-integrated automation to disable or block the identity immediately under defined conditions.

Disabling the account should not be treated as complete containment. Active sessions, tokens, privileged roles, application passwords, VPN sessions, API credentials, and customer-specific accounts may require additional action depending on the architecture.

Verification includes confirming that the intended access paths are no longer usable and checking whether the attacker or user created alternate persistence before the account was disabled.

23.55 Who Can Approve an Emergency Firewall Change?

Emergency firewall changes are necessary when the organization must block malicious traffic, isolate a network segment, restore a critical service, or respond to an unexpected threat. The danger is that emergency changes can bypass normal review and become permanent.

Harbor Point and NorthStar should define emergency authority in advance. NorthStar may be authorized to block a confirmed malicious IP address or isolate a compromised segment without waiting for ordinary change approval. Broader changes that could interrupt production may require an on-call customer decision unless immediate harm justifies pre-authorized containment.

Every emergency change should receive retrospective review. The team verifies the rule, documents its purpose, determines whether it remains necessary, removes temporary rules when the emergency ends, and updates diagrams or baselines if the permanent architecture changed.

The evidence should show that emergency authority accelerated protection without eliminating governance.

23.56 What If the Customer Cannot Be Reached?

A managed-security relationship needs an answer to this question before the first emergency. If Harbor Point cannot be reached, NorthStar and Beacon should not improvise authority from memory. The contract, incident plan, and emergency procedures should define what protective actions are permitted.

A sensible model identifies actions that can occur automatically or under provider judgment, actions that require customer approval, and an escalation ladder with multiple contacts. It can also distinguish reversible protective actions from irreversible or high-impact actions.

For example, isolating a suspicious employee laptop may be pre-authorized because it is reversible and limits potential harm. Shutting down a production engineering environment may require a higher threshold. The exact model belongs to Harbor Point's risk and business decisions.

When the customer is unavailable, every attempted contact and action should be documented. Once contact is restored, the provider explains what occurred and confirms the next steps.

23.57 How Are Emergency Decisions Documented Before the Emergency?

The organization records emergency authority in the incident-response plan, service agreement, responsibility matrix, escalation matrix, or associated operating procedures. The exact document matters less than clarity and consistency across the documents people actually use.

The procedure should identify roles rather than depending only on individual names. It should include current contact information separately so personnel changes do not require rewriting the entire policy. It should identify severity thresholds, permitted containment actions, notification expectations, and any systems requiring special handling.

Tabletop exercises validate the documentation. A written procedure can appear clear until participants simulate a 2:00 a.m. ransomware event and discover that the SOC does not have the MSP's after-hours number or that nobody knows whether the MSP may isolate a domain controller.

The exercise record becomes evidence that the organization tested its coordination model and corrected identified weaknesses.

23.58 How Do We Know the Continuous-Readiness Process Itself Is Working?

A process can exist on paper and still fail operationally. Harbor Point therefore needs measures that test the readiness system itself. Are exceptions discovered promptly? Are tickets assigned? Do critical items age without action? Are missing agents reconciled? Are restore tests completed? Are access reviews producing removals? Are documentation updates occurring after major changes?

One useful measure is the age of unresolved high-risk exceptions. Another is the percentage of expected assets reconciled across security systems, accompanied by the

actual unexplained exceptions. Another is the number of failed control-health conditions that were detected by monitoring rather than by accident.

The organization should also perform sampled operational tests. Select a recent terminated employee and trace offboarding. Select a new laptop and verify every required protection. Select a firewall change and trace authorization through implementation and validation. Select an incident and trace escalation and lessons learned.

These tests answer a stronger question than whether a policy exists: can the organization demonstrate that the process produces the intended result?

23.59 What Is Evidence Decay?

Evidence decay occurs when an artifact becomes less useful for describing the current security state as time passes or the environment changes. A screenshot of an MFA policy taken during last year's assessment may remain historically accurate, but it cannot establish that today's policy is identical. A network diagram can become stale when a new server or provider is added.

Different evidence decays at different rates. A corporate policy may remain current for a year if the organization and requirement do not change. A list of privileged administrators can become stale the moment a new administrator is added. A vulnerability scan can become outdated when new vulnerabilities are disclosed or systems change.

The evidence strategy should therefore classify evidence by purpose. Historical evidence demonstrates that a process operated at a prior time. Current-state evidence demonstrates present configuration or population. Periodic evidence demonstrates repeated operation. Event evidence documents a specific change or incident.

Understanding decay prevents the organization from presenting a beautiful archive that no longer describes reality.

23.60 How Much Evidence Is Enough?

More evidence is not automatically better. Thousands of screenshots can make the important story harder to understand and create storage, sensitivity, and maintenance problems. The goal is sufficient, authoritative evidence that demonstrates the implementation and operation being claimed.

For a technical control, the strongest package may combine a documented procedure, current configuration or system record, population or scope information, and a sample of operational records. For example, endpoint protection can be demonstrated

by the policy, current agent population, reconciliation against inventory, and selected remediation tickets for exceptions.

The organization should avoid creating evidence solely because it looks impressive. Every retained artifact should answer a question. What claim does this prove? What time period does it cover? What system produced it? Who can explain it? Is it authoritative?

Evidence curation is therefore part of readiness. The goal is a coherent story, not a warehouse of screenshots.

23.61 What Happens When the Evidence Platform Changes?

When NorthStar replaces RMM, Beacon replaces SIEM, or Harbor Point changes an identity or ticketing platform, historical evidence can become difficult to retrieve. The migration plan should therefore identify records that may be needed after the old system is retired.

The team determines what history is operationally or contractually necessary, how long it must remain available, whether exports preserve sufficient context, and who will be able to retrieve it. A CSV containing raw events may not replace a searchable investigation record if important analyst notes are lost.

The new platform should also be tested for evidence generation. Can Harbor Point still demonstrate asset coverage? Can NorthStar show patch history? Can Beacon retrieve incident records? Can audit logs identify administrative actions?

Technology replacement is complete only when the security function and its evidence function both survive the transition.

23.62 How Does a Configuration Baseline Work in Practice?

A baseline is a documented or technically represented expected state. It may include operating-system settings, firewall rules, identity policies, device-management profiles, security-agent configuration, approved software, or cloud settings. The baseline gives the organization something against which change can be understood.

Harbor Point does not need to freeze every setting forever. Baselines evolve through controlled change. If NorthStar determines that a stronger endpoint policy is appropriate, the change is tested, approved according to the operating model, deployed, verified, and then becomes part of the new expected state.

Monitoring compares actual state with expected state. Some platforms enforce the baseline automatically; others report deviations. A deviation opens investigation. Was

the difference an approved change not yet reflected in the baseline, a temporary exception, a software update, a failed deployment, or unauthorized modification?

The result should be either restoration to the baseline or an intentional update of the baseline. Leaving unexplained differences indefinitely defeats the purpose.

23.63 How Does Drift Appear in Microsoft 365 Government?

Cloud drift can be subtle because administrators can change settings quickly through portals, scripts, APIs, or automation. A new Conditional Access exclusion, guest-sharing setting, application consent, privileged-role assignment, mailbox forwarding rule, or Intune policy exception can alter the security model without changing any physical equipment.

NorthStar and Harbor Point therefore need change visibility. Audit logs, role reviews, configuration exports, policy comparisons, and service-management records help connect cloud changes to authorization. Significant changes should be reviewed for documentation impact.

Service-provider changes create another kind of drift. Microsoft may introduce or retire functionality. The organization should distinguish a vendor service change from an administrator change and evaluate whether the new behavior affects its security design.

The continuous-readiness question remains the same: does the live tenant still operate according to the approved security model, and can the team explain meaningful differences?

23.64 How Does Drift Appear in Endpoint Management?

An endpoint can drift when a user installs unauthorized software, a policy fails, encryption becomes suspended, EDR stops reporting, a local administrator is added, the device misses patches, or management enrollment breaks. The laptop can remain usable while security gradually deteriorates.

Device-management and security platforms can report many of these conditions, but the organization must define which deviations are actionable. A stale device may be retired, traveling, offline, or unmanaged. Investigation provides the context.

NorthStar should connect device-health exceptions to tickets and resolution. If Priya's laptop is missing an EDR sensor, the goal is not merely reinstalling the agent. The team asks why the build or health-monitoring process allowed the condition and whether other devices could have the same problem.

Periodic reconciliation across inventory, device management, RMM, EDR, vulnerability management, and patching exposes silent endpoint drift.

23.65 How Does Drift Appear in Firewalls and Networks?

Network drift often appears as accumulated rules, temporary access, obsolete VPN accounts, undocumented routes, new wireless networks, or equipment replaced without updating diagrams and monitoring. Because networks are foundational, small changes can create new paths between systems.

A firewall review should not consist solely of reading thousands of rules. The team focuses on recent changes, broad permissions, temporary rules, unused rules, administrative access, remote-access configuration, logging, and alignment with the current architecture.

When an unexplained rule is found, NorthStar traces the audit log and change tickets. If the rule was legitimate but undocumented, the process failed even if the technical configuration is acceptable. If the rule is no longer required, it is removed and the result verified.

Network diagrams and firewall configurations should tell the same story at an appropriate level of detail.

23.66 What Does Good Vulnerability Prioritization Look Like?

A vulnerability score is an input, not a complete decision. Harbor Point and NorthStar consider whether the vulnerable asset is exposed, whether exploitation is known, whether the system handles CUI, what privileges are required, whether compensating controls exist, and what business function would be affected by remediation.

This allows the team to distinguish urgency without using severity as an excuse for delay. A critical vulnerability on an unused isolated lab machine may be less urgent than a lower-scored weakness on an Internet-facing authentication service. The reasoning should be documented for significant exceptions.

Prioritization also determines escalation. A technician can remediate ordinary findings. A vulnerability requiring production downtime, architecture change, or risk acceptance moves to Harbor Point management.

Verification closes the decision. The finding should not disappear merely because a ticket says patched. The team confirms that the vulnerable condition no longer exists or that the approved mitigation is actually effective.

23.67 What If There Is No Patch?

Sometimes a vendor has not released a fix, the product is unsupported, or the patch cannot be installed immediately. Continuous readiness does not allow the organization to pretend the vulnerability does not exist. It requires an explicit risk treatment.

NorthStar and Harbor Point examine mitigations: disabling the vulnerable feature, restricting network access, changing configuration, increasing monitoring, isolating the system, removing the software, upgrading the product, or accelerating replacement. The appropriate choice depends on the vulnerability and business function.

The condition remains tracked. A temporary mitigation is not automatically permanent remediation. The team monitors vendor guidance and revisits the exception until the underlying risk is resolved or the system is retired.

Evidence should show awareness, decision, mitigation, ownership, review, and eventual closure.

23.68 How Should Backup Testing Be Scheduled?

Recovery testing should reflect business importance and change. A critical engineering service may require more frequent or deeper testing than an archive with low recovery urgency. Major platform changes, migrations, or backup-product changes can trigger additional tests because the recovery assumptions changed.

Harbor Point first defines recovery expectations. NorthStar then designs tests that prove those expectations. A monthly file restore may verify basic recoverability, while a quarterly application recovery exercise may validate dependencies. An annual broader exercise may test people, documentation, communications, and alternate infrastructure.

The schedule should not become a ritual. If every test restores the same easy file, the organization learns very little. Test selection should rotate through meaningful scenarios and occasionally challenge assumptions.

Failed tests are documented and repeated after correction. A failed test that produces improvement is more valuable than a ceremonial test designed to guarantee success.

23.69 What Does a Monthly Customer Security Review Actually Sound Like?

NorthStar's service manager meets with Harbor Point's accountable contact. The meeting begins with exceptions rather than a product tour. Three endpoints are outside the expected vulnerability population, one privileged account is awaiting removal, two critical vulnerabilities exceeded the target remediation window, and the previous month's restore test identified a documentation gap that has now been corrected.

The service manager explains what each condition means, what has already been done, what remains, and which decisions Harbor Point must make. Harbor Point asks whether the missing endpoints contain CUI, whether the vulnerabilities affect production, and whether the privileged account belongs to an active vendor.

The meeting also reviews significant changes: new systems, providers, CUI flows, incidents, major Microsoft 365 changes, and upcoming projects. The purpose is to connect technical operations to business change.

The resulting record captures decisions and owners. Continuous readiness is strengthened because management sees unresolved conditions before they become assessment surprises.

23.70 What Should a Quarterly Privileged-Access Review Actually Do?

The reviewer begins with the current privileged population, not last quarter's spreadsheet. Identity platforms, RMM, firewalls, backup, security tools, cloud services, and customer-specific systems are examined according to the architecture.

Each assignment is challenged against current job need. Does Maria still support Harbor Point? Does a vendor still require tenant administration? Does an emergency account remain correctly protected? Is a service identity being used interactively? Are any shared accounts still present?

Changes are executed and verified. The review record identifies who reviewed, what was removed or retained, and why. If the review discovers that a departed technician retained access, the team treats that as a process failure and investigates how offboarding missed the account.

The objective is not quarterly paperwork. It is reduction of accumulated authority.

23.71 What Should an Annual Readiness Review Actually Do?

The annual review brings together the year's operating evidence and asks whether the security program still describes the organization. Harbor Point reviews contracts and CUI flows, major architecture, external providers, SSP, policies, responsibility assignments, assessment scope, significant incidents, open exceptions, recovery results, and recurring control-health trends.

NorthStar contributes technical evidence and identifies persistent operational problems. Beacon contributes monitoring and incident trends. Management examines whether recurring exceptions indicate underfunding, architecture weakness, unclear ownership, or unrealistic procedures.

The review should also validate the evidence mechanism itself. Can the team retrieve records from the beginning of the year? Did platform migrations preserve needed history? Are current contacts and escalation paths accurate? Can sampled users, devices, and changes be traced through the expected processes?

Where an annual affirmation is applicable under current CMMC requirements, the year's operating discipline provides the factual foundation for the affirming official's process rather than forcing a last-minute reconstruction.

23.72 How Do We Handle a New Subcontractor Receiving CUI?

The project team should not begin by emailing files and asking security afterward. The proposed subcontractor relationship should trigger contracting and security review before CUI flows. Harbor Point determines what information will be shared and what contractual requirements apply.

The technical review determines the approved transfer method, recipient identities, systems and providers involved, access lifecycle, and whether Harbor Point's architecture or scope documentation changes. NorthStar may configure the approved exchange mechanism and identity controls.

The current DFARS 252.204-7021 clause, when included and applicable, contains CMMC flowdown and subcontractor status requirements. Because contract applicability and CMMC implementation are time-sensitive, Harbor Point should evaluate the actual contract and current rules rather than relying on a generic assumption.

After the relationship ends, access and exchange mechanisms are reviewed and removed as appropriate. The provider relationship has a lifecycle just like an employee identity.

23.73 How Do We Handle a Microsoft Service Change?

Cloud vendors continuously evolve services. A service change can affect interfaces, authentication, APIs, logging, security defaults, or feature availability. The first challenge is determining which changes matter to Harbor Point rather than reacting to every vendor announcement.

NorthStar monitors relevant service communications and maps them to the customer's architecture. A change affecting a feature Harbor Point does not use may require no action. A change affecting authentication, logging, device management, or a critical integration deserves analysis.

Where testing is possible, NorthStar validates the change in a controlled way. It updates scripts, procedures, integrations, or training as needed. If the change materially alters how a security requirement is implemented, Harbor Point reviews documentation.

The evidence is the change record and validation, not a collection of every vendor bulletin.

23.74 How Do We Handle an RMM Migration Without Losing Control?

Before migration, NorthStar establishes the authoritative device population and exports the operational information it may need from the old platform. It inventories scripts, policies, technician roles, API integrations, automation, customer groups, and security logging.

During migration, the greatest danger is ambiguity. Some devices may be controlled by the old agent, some by the new, and some by both or neither. NorthStar uses reconciliation to track each device through the transition. Automation is constrained until targeting is verified.

After migration, the old environment is deliberately dismantled. Agents are removed, API tokens revoked, technician access disabled, old automation stopped, and historical records preserved according to the evidence plan. The new platform's security settings and customer separation are reviewed.

Harbor Point does not need to manage the migration, but it should understand that a major administrative control plane changed and receive assurance that coverage and evidence remained intact.

23.75 How Do We Handle a Failed Restore Test Without Hiding It?

A failed restore test is not an embarrassment to be removed from the evidence library. It is exactly the kind of controlled discovery a mature program wants. The organization found a recovery weakness before a real disaster.

The record should explain the intended test, failure point, cause, business consequence, corrective action, and retest. If the failure reveals that the backup scope omitted a dependency, the asset and recovery architecture are corrected. If credentials were unavailable, credential management is corrected.

Management should distinguish a failed test that is promptly corrected from a neglected recovery weakness. The first demonstrates an effective assurance process; the second demonstrates unresolved risk.

The final evidence package can show both the initial failure and successful retest because together they demonstrate learning and verification.

23.76 How Do We Handle a Role Change Without Creating Privilege Creep?

Daniel moves from advanced engineering to project management. The easy action is adding his project-management permissions. The correct lifecycle also reviews what engineering access should be removed.

Harbor Point's manager identifies the new business role. NorthStar or the internal administrator changes groups and application permissions according to that authorization. Privileged or exceptional access receives special review. The team verifies both addition and removal.

Role-change workflows are important because privilege creep is usually not caused by malicious intent. It is caused by additive administration: every new responsibility adds access while old access is rarely removed.

Evidence connects the management decision to the resulting access state.

23.77 How Do We Handle a Replacement Laptop Correctly?

Priya's replacement laptop is not ready merely because Windows starts and Microsoft 365 opens. It must enter the same controlled lifecycle as any new endpoint. The asset is recorded, assigned to Priya, enrolled in management, encrypted, protected by EDR, added to RMM, included in vulnerability and patch processes, configured with approved software, and validated against access policies.

The old laptop also has a lifecycle. Harbor Point removes or protects data, removes the device from active access where appropriate, retires management records correctly, and disposes of or reuses the hardware according to procedure.

Reconciliation catches incomplete transitions. If both old and new devices remain active indefinitely, the team investigates. If the new device appears in Intune but not EDR, onboarding is incomplete.

The replacement event therefore tests both provisioning and retirement controls.

23.78 How Do We Handle a Security Incident Six Months After Assessment?

Beacon detects suspicious PowerShell behavior on a Harbor Point workstation. The assessment six months earlier demonstrated that endpoint monitoring and incident response existed. The current event tests whether those capabilities still operate.

Beacon validates the alert and correlates identity and network events. Under the pre-agreed authority model, the workstation is isolated. NorthStar identifies the user, device, recent changes, patch state, and management history. Harbor Point's incident contact is notified according to severity.

The investigation determines whether credentials were compromised, whether other systems show related behavior, and whether CUI may have been affected. Containment, eradication, recovery, reporting analysis, and evidence preservation follow the incident plan and applicable obligations.

Afterward, the team identifies lessons. Perhaps the event exploited an approved scripting tool, revealing a need for better behavioral detection rather than simple software blocking. Perhaps the investigation was delayed because one log source had insufficient retention. Those lessons become controlled improvements.

23.79 What Does Root-Cause Analysis Mean in an MSP Environment?

Root-cause analysis asks why the condition was possible, not merely which technician touched the system last. If a server missed EDR, the immediate cause may be that the agent was not installed. The deeper cause may be that server provisioning had no security gate and no reconciliation rule.

Good analysis separates human error from system design. People will occasionally forget steps. A mature process is designed to detect predictable mistakes before they become long-lived security gaps.

The corrective action therefore operates at two levels. NorthStar fixes the server today and improves the provisioning or monitoring process for tomorrow. Harbor Point may need to change approval or project procedures if systems can enter production without security review.

Evidence of root-cause improvement is especially valuable because it shows that the organization learns from operational failures.

23.80 How Do We Know Documentation Matches Reality?

Documentation validation should use samples from the live environment. Select a network segment from the diagram and compare it with actual routing and firewall configuration. Select a provider in the SSP and verify the current service and responsibility. Select an asset category and confirm that the inventory and control descriptions match what technicians actually operate.

Interviews are also useful. Ask Maria how she onboards a Harbor Point laptop and compare the answer with the written procedure. If the procedure says one thing and the technician consistently does another, the organization must determine which is correct.

Documentation drift can reveal that the process is obsolete, that technicians are bypassing it, or that the environment changed without governance. Correcting the document alone may hide the real problem.

The objective is not perfect prose. It is trustworthy operational documentation.

23.81 What Does a Random Tuesday Test Look Like?

Harbor Point chooses an ordinary day with no assessment scheduled. Management asks NorthStar to demonstrate the current managed endpoint population and identify any systems missing EDR. NorthStar produces the inventory comparison and explains the exceptions.

Next, Harbor Point selects a recently terminated user and traces offboarding across identity, VPN, SaaS, and privileged systems. It selects a recent firewall change and traces request, approval, implementation, and verification. It asks Beacon to demonstrate that expected log sources are active and to retrieve a recent investigation record.

Finally, the team chooses a protected system and asks how it would be restored. It reviews the last test and confirms that the current runbook includes dependencies.

The exercise is not a mock assessment designed to frighten employees. It is a health check. Any question that requires frantic reconstruction becomes an improvement item.

23.82 The Twelve-Month Harbor Point Story - January: Two Employees Leave

In January, two Harbor Point employees leave on the same Friday. One is a standard user; the other has elevated engineering permissions. Human Resources sends the authorized termination event. The identity workflow disables accounts at the appropriate time, revokes sessions, removes group and privileged access, and creates device-return tasks.

NorthStar discovers that the privileged employee also had a direct account in a legacy engineering application that was not federated with Entra ID. The account appears on the application-access inventory and is disabled. This validates why offboarding cannot rely solely on the central identity provider.

The monthly review samples the termination and confirms completion. The legacy application is added to an automated or procedural offboarding dependency list so future terminations do not depend on technician memory.

23.83 The Twelve-Month Harbor Point Story - February: Priya Receives a Replacement Laptop

Priya's old laptop has a failing battery and is replaced. The new device follows the controlled build and is reconciled across inventory, Intune, RMM, EDR, vulnerability management, and patching before CUI access is enabled.

The old device remains in EDR for several days after retirement. Rather than deleting the record immediately, NorthStar confirms the device is physically returned and no longer active. It then retires the management records according to procedure.

The event produces ordinary evidence: asset assignment, configuration status, security-agent coverage, access authorization, and retirement record. No assessment-specific screenshot is required.

23.84 The Twelve-Month Harbor Point Story - March: A Critical Vulnerability Appears

A vendor announces a critical vulnerability in software used on three engineering servers. NorthStar identifies the affected versions through inventory and vulnerability data. Beacon reviews for relevant indicators of exploitation.

The vendor patch requires a reboot. Harbor Point cannot interrupt a critical simulation until evening, so management approves a short remediation window and temporary network restriction. NorthStar patches the servers, verifies versions and vulnerability status, and removes the temporary restriction after validation.

The complete story is visible in the advisory, asset analysis, change ticket, business approval, mitigation, patch record, verification, and closure.

23.85 The Twelve-Month Harbor Point Story - April: A New Subcontractor Receives CUI

Harbor Point wins work requiring collaboration with a new subcontractor. Contracting identifies that protected information will be shared before the project begins. Security reviews the relationship and current applicable requirements.

NorthStar configures the approved exchange path and access. Harbor Point authorizes named users and determines what information can be shared. The information-flow diagram, provider or subcontractor records, and relevant SSP material are reviewed.

The relationship enters a lifecycle with periodic access review and an expected project end. The organization avoids creating an indefinite external access path simply because the first transfer succeeded.

23.86 The Twelve-Month Harbor Point Story - May: Microsoft Changes a Service

Microsoft announces a change affecting an authentication or management feature Harbor Point uses. NorthStar determines that the change applies to the government environment and could affect an integration.

The team tests the integration, updates the configuration, and confirms that authentication, logging, and expected operations continue. The change is recorded because it affects a security-relevant technical dependency.

Harbor Point does not need to understand every API detail, but it receives confirmation that the change was evaluated and did not silently break the operating control.

23.87 The Twelve-Month Harbor Point Story - June: Beacon Investigates an Incident

Beacon detects suspicious activity on an endpoint. The established escalation model works: the endpoint is isolated under pre-authorized conditions, NorthStar supports technical containment, and Harbor Point receives management notification.

The investigation finds no confirmed CUI exfiltration, but it reveals that a browser extension installed by the user contributed to the event. Harbor Point updates its software and extension governance, NorthStar improves technical restrictions where feasible, and user training is refreshed.

The incident therefore changes the program rather than becoming an isolated closed ticket.

23.88 The Twelve-Month Harbor Point Story - July: Recovery Testing Fails

NorthStar performs a planned recovery test for an engineering service. The server restores, but the application cannot start because a license dependency was missing from the runbook.

The team records the failure, adds the dependency, validates credentials and restoration order, and repeats the exercise successfully. Management learns that the backup system was healthy but the recovery design was incomplete.

The failed test becomes evidence of an effective assurance process because the weakness was discovered, corrected, and verified before a real disaster.

23.89 The Twelve-Month Harbor Point Story - August: NorthStar Replaces RMM

NorthStar migrates Harbor Point from the old RMM to a new platform. The migration plan tracks every expected device, technician role, script, automation, integration, and historical record.

During reconciliation, one rarely used engineering laptop appears in inventory but in neither RMM platform. Investigation finds that it was offline throughout migration. NorthStar contacts Harbor Point, brings the device online, installs and validates the new agent, and confirms EDR and patch health at the same time.

The migration is not closed until old agents and access are removed and the expected population is reconciled.

23.90 The Twelve-Month Harbor Point Story - September: Daniel Changes Roles

Daniel moves from engineering into project management. Management authorizes the new role. The access workflow adds project-management resources and reviews old engineering groups, privileged access, and application permissions.

One old engineering group is intentionally retained for a thirty-day transition and documented with an expiration review. At the end of the period, NorthStar removes it and verifies access.

This prevents the common pattern in which role changes only add permissions.

23.91 The Twelve-Month Harbor Point Story - October: A Patch Exception Ages

An engineering application cannot support a required operating-system update until the vendor certifies compatibility. The exception was originally approved for thirty days with network restrictions and increased monitoring.

At the review date, the vendor still has not certified the patch. Harbor Point does not simply extend the exception automatically. NorthStar provides current exposure and vendor information, Beacon reports whether related threat activity has been observed, and management decides whether to extend, isolate further, accelerate application replacement, or accept downtime for testing.

The renewed decision receives a new review point. The exception remains visible rather than becoming permanent through neglect.

23.92 The Twelve-Month Harbor Point Story - November: A Guest Account Is Found

A quarterly guest-access review finds an external user whose project ended months earlier. The account has not recently accessed data, but its continued presence is unexplained.

Harbor Point confirms the business relationship ended. NorthStar removes access and checks whether the guest belonged to other groups or sites. Audit information is reviewed as appropriate.

The team asks why project closeout did not trigger guest removal and updates the project-offboarding workflow. The discovery becomes a process improvement, not merely an account deletion.

23.93 The Twelve-Month Harbor Point Story - December: The Annual Readiness Review

At year end, Harbor Point does not begin by asking whether it can find enough screenshots. It reviews the year's changes and asks whether the current environment, documentation, responsibilities, and evidence still align.

The January terminations, February device replacement, March vulnerability, April subcontractor, May cloud change, June incident, July recovery failure, August RMM migration, September role change, October exception, and November guest review are all visible through normal records.

Open exceptions are identified. The SSP and diagrams are compared with reality. Privileged access is reviewed. Provider responsibilities are confirmed. Evidence retention is tested. Current regulatory and contractual requirements are reviewed before any required affirmation or assessment activity.

The year's history demonstrates the central principle: readiness was maintained by absorbing change, not by preventing change.

23.94 What If Harbor Point Had Done None of This?

Imagine the same year without continuous readiness. The departed privileged employee still has a legacy account. Priya's old laptop remains active in management. The March vulnerability is patched on two servers but missed on the third. The subcontractor receives CUI through an improvised transfer service. The Microsoft change silently breaks a logging integration. The browser extension incident is closed without changing policy.

The recovery weakness remains undiscovered until a real outage. The RMM migration misses the offline laptop. Daniel accumulates both old and new permissions. The patch exception remains indefinitely. The guest account survives. The SSP still describes last year's environment.

Nothing in this scenario requires a dramatic malicious act. The program deteriorates through ordinary business activity. That is why continuous readiness is necessary.

23.95 How Should a New MSP Technician Learn This Program?

A new technician should not be handed only a list of CMMC acronyms. Training should begin with the customer architecture and the reason behind the controls. The technician learns what information Harbor Point protects, which systems are in the

managed environment, which actions are routine, which require approval, and how escalation works.

Then the technician learns the tools in context. RMM is not merely remote-control software; it is a high-authority management plane. EDR is not merely another agent; it supports detection and response. Tickets are not clerical overhead; they preserve authorization and evidence. Customer separation is not a naming convention; it limits cross-customer blast radius.

Practical exercises should require the technician to onboard a test device, investigate a missing agent, process a patch exception, retrieve evidence, and respond to a simulated Beacon escalation. Competence is demonstrated through operation, not vocabulary.

This training model makes continuous readiness part of technician culture rather than a specialized compliance function.

23.96 What Should Management Understand Without Becoming Technicians?

Management does not need to know every PowerShell command or firewall syntax. It does need to understand what the security program depends upon, which exceptions remain open, which decisions require business authority, and whether providers are performing assigned responsibilities.

A useful management conversation translates technical conditions into consequences. 'Three EDR agents are stale' becomes 'three expected endpoints are not currently providing the security visibility we require, and two have been restored while one employee is traveling.' 'One critical vulnerability is overdue' becomes 'the vendor application cannot yet accept the patch; network restrictions are in place and management must decide whether to extend the exception or accelerate replacement.'

This level of understanding supports informed affirmation, risk decisions, budgeting, staffing, and provider oversight without turning executives into console operators.

23.97 How Should the MSP Prove Its Own Processes Work?

NorthStar should test the services it provides rather than relying only on customer assessments to expose weaknesses. It can sample customer offboarding, verify RMM customer separation, test backup escalation, review privileged technician access, validate vulnerability-ticket integration, and simulate loss of a monitoring source.

Internal quality review should look for systemic patterns. If multiple customers have stale EDR agents after laptop replacement, the issue may be NorthStar's provisioning process rather than separate customer mistakes.

An MSP that learns across customers can improve its standard operating model while preserving customer-specific requirements. This is one of the advantages of mature managed service, provided standardization does not erase customer-specific responsibility.

Evidence of internal assurance also helps the MSP explain to customers how it maintains the services on which their security programs depend.

23.98 How Do Contractor and MSP Continuous-Readiness Calendars Fit Together?

Harbor Point and NorthStar should not maintain two unrelated calendars. NorthStar's operational cycles feed Harbor Point's governance cycles. Daily and weekly technical exceptions become monthly service-review information. Monthly trends feed quarterly management decisions. Quarterly changes and evidence support annual program validation.

Harbor Point also contributes events that cannot originate from an MSP dashboard: new contracts, employee role decisions, subcontractors, acquisitions, business-process changes, and information-sharing relationships. Those events enter the same readiness system.

The result is a two-way operating model. Technical monitoring informs business governance, and business change informs technical security. Continuous readiness fails when either side operates alone.

23.99 What Is the Final Test Before We Call the Program Continuously Ready?

The final test is not perfection. The organization asks whether it knows its current environment, knows its meaningful exceptions, knows who is responsible, can detect control degradation, can respond to change, can retrieve evidence, and can explain how its documented program matches reality.

Harbor Point should be able to select a user, device, system, provider, vulnerability, change, incident, or recovery test and trace the relevant lifecycle without inventing the story afterward. NorthStar should be able to demonstrate its assigned technical processes. Beacon should be able to demonstrate monitoring and escalation for its assigned scope.

Where the answer is incomplete, the organization has found work to do. That discovery is part of readiness, not evidence that the program has failed. A mature program makes weaknesses visible while there is still time to correct them.

Continuous readiness is therefore an operating capability: the ability to remain aware of the current state, absorb change, detect degradation, correct failures, verify results, and preserve trustworthy evidence.

23.100 Closing Principle - The Assessment Is a Milestone; Operations Are the Program

The assessment is important because it tests whether the organization can demonstrate required security outcomes. But the assessment is not the activity that protects Harbor Point on an ordinary Tuesday. The protection comes from identity administration, endpoint management, monitoring, patching, vulnerability response, backup and recovery, controlled change, provider coordination, incident response, documentation, and management decisions performed correctly over time.

NorthStar's value is not that it can prepare screenshots before an assessor arrives. Its value is that it can operate assigned security functions consistently enough that evidence exists because the work happened. Beacon's value is not that it can show a SIEM dashboard. Its value is that meaningful security events and loss of visibility are detected, investigated, and escalated. Harbor Point's responsibility is not satisfied by hiring those providers. It must govern the environment, authorize business decisions, understand its obligations, and verify that shared responsibilities function.

When these pieces operate together, the next assessment is not a rescue project. It is another opportunity to demonstrate a security program that has been functioning all along.

Normal operations should create security. Normal operations should create evidence. Normal operations should maintain readiness.

Current Regulatory Note for This Edition

This chapter distinguishes durable continuous-readiness practices from time-sensitive CMMC implementation details. As reviewed on September 22, 2026, the Department of Defense Chief Information Officer CMMC site states that the planned Phase II requirements were suspended on July 13, 2026 and that Phase I self-assessment requirements remain in place. The same official page describes Level 1 as an annual self-assessment with annual affirmation and Level 2 self-assessment as a three-year assessment cycle with annual affirmation. Because implementation policy can

change, contractors should verify the current DoD CMMC materials and the clauses in the contract at issue before relying on an implementation schedule.

Current DFARS 252.204-7021 defines a current Final Level 1 self-assessment status as not older than one year, and Final Level 2 self-assessment and C3PAO statuses as not older than three years, in each case subject to the clause conditions concerning changes in compliance and current affirmation. When the clause applies, it requires the contractor to have and maintain the required current CMMC status for covered contractor information systems for the duration of the contract and to complete and maintain an annual affirmation of continuous compliance in SPRS for each applicable CMMC UID. These regulatory statements should be rechecked during whole-book production and before future editions are published.

Authoritative Sources for Current CMMC Statements

Department of Defense Chief Information Officer, Cybersecurity Maturity Model Certification - About CMMC: https://dodcio.defense.gov/CMMC/About/

Acquisition.gov, DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025): https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements.

Acquisition.gov, DFARS Subpart 204.75, Cybersecurity Maturity Model Certification: https://www.acquisition.gov/dfars/subpart-204.75-cybersecurity-maturity-model-certification

Chapter 24
Building a CMMC Program from Day One

CMMC for MSPs: From Readiness to Certification
Authored by Dr. Charles Edwards

24.1 The Day-One Question

A contractor can read hundreds of pages about CMMC and still arrive at a practical question on Monday morning: where do we begin? The answer is not to buy a compliance platform, order a penetration test, migrate immediately to a government cloud, or begin writing policies copied from another company. Day One begins with understanding the business, the information, the contracts, and the environment that must be protected.

This chapter follows two organizations in parallel. The first is Redwood Precision Systems, a fictional small defense contractor that has grown from commercial engineering work into federal and defense work. The second is Summit Ridge Technology Services, its fictional MSP. Redwood understands engineering and its customers, while Summit Ridge understands the systems it manages. Neither organization can build the program alone because neither possesses the entire picture.

The implementation journey will use four connected stages. Phase One is readiness and compliance design. Phase Two is technical implementation. Phase Three is validation, knowledge transfer, and operational handoff. After those implementation phases comes the permanent operating state: continuous readiness. The phases are separated for teaching, but in a real project they overlap and feed one another.

24.2 Before Anything Else: Determine Why CMMC Matters to This Organization

Redwood should begin with its contracts, solicitations, flowdowns, and the information it receives or creates for government work. The organization must distinguish a general desire to improve cybersecurity from a contractual requirement that invokes particular safeguarding and assessment obligations. This prevents the technology team from designing an expensive environment around assumptions.

The contracting function and security function should work together. Contract personnel identify clauses and customer requirements. Program managers explain what work will be performed. Technical personnel explain which systems support that work. Management decides what business the company intends to pursue. Those conversations establish the purpose of the CMMC program.

As of September 2026, DoD's official CMMC information states that implementation is paused in Phase I and that Phase I self-assessment requirements remain in place. Current DFARS 252.204-7021 also contains requirements concerning current CMMC status, annual affirmation, applicable information systems, and flowdown when the clause applies. These details are time-sensitive. Redwood therefore checks its actual

contract and the current authoritative rules instead of designing from an old slide deck or consultant memory.

24.3 Plain English First: FCI, CUI, and Why Information Drives the Architecture

Federal Contract Information, or FCI, is information provided by or generated for the Government under a contract that is not intended for public release, subject to the regulatory definition and exclusions. Controlled Unclassified Information, or CUI, is information that requires safeguarding or dissemination controls under applicable law, regulation, or government-wide policy. For a beginner, the important lesson is that these labels affect what the organization must protect and therefore which systems, people, and providers become relevant.

Redwood should not start by asking which computers are 'CMMC computers.' It should start by asking where protected information comes from, who receives it, what they do with it, where they save it, how they send it, how they print it, whether it enters engineering tools, whether it is backed up, and which external services touch it. The systems emerge from the information flow.

An engineering drawing may arrive through an approved portal, be downloaded to a managed workstation, opened in a CAD application, saved to a file service, discussed in collaboration software, included in backup, and transmitted to an authorized subcontractor. Each step reveals technology and responsibility that a device-only inventory can miss.

24.4 Build the Information-Flow Story Before the Technology Shopping List

The first practical workshop should place contracting, program management, engineering, IT, and security in the same conversation. Redwood chooses representative government work and traces information from receipt through use, storage, transmission, archival, and disposition. The team records people, systems, locations, applications, external providers, and transfer methods.

The purpose is not to create a beautiful diagram on the first attempt. The purpose is discovery. An engineer may reveal that large files are exchanged through a service IT did not know existed. A project manager may reveal that a subcontractor receives drawings by email. The MSP may reveal that backups are stored with an external provider. Those discoveries are precisely why the workshop exists.

Summit Ridge contributes technical facts but should not decide what information is CUI on its own. Redwood supplies contractual and business context. Where classification or marking questions remain uncertain, Redwood obtains appropriate authoritative clarification. The MSP should not invent a legal or contractual answer because it happens to administer the server.

24.5 Create the First Scope Model

Scope is the boundary around the people, technologies, facilities, and services relevant to the CMMC assessment and the protection of the applicable information. A beginner often assumes the safest approach is to include the entire company. That may be workable for some organizations, but it can also create unnecessary complexity. Another organization may deliberately segment the CUI environment so that only a controlled population participates.

Redwood compares possible architectures. A broad enterprise scope may be simpler conceptually because employees use one environment, but it can increase the number of systems and users that must meet the required security model. A segmented enclave can reduce scope, but it introduces boundary controls, user workflow, data-transfer rules, and operational complexity. There is no universal architecture that is correct for every contractor.

The decision should be driven by business workflow, security, contractual requirements, maintainability, and cost over time. The cheapest migration project is not necessarily the cheapest operating model. If employees constantly need to move information across a poorly designed boundary, the organization may create shadow workflows that defeat the intended segmentation.

24.6 Asset Inventory: Know What Exists Before You Protect It

Once the preliminary scope is understood, Redwood creates an authoritative asset inventory. The inventory is more than a spreadsheet of serial numbers. It should support decisions about what the asset does, who owns it, where it resides, what information it handles, how it is managed, and which protections apply.

Summit Ridge can export device populations from RMM, EDR, device management, vulnerability scanning, backup, and directory services. Those exports are discovery inputs, not automatically the authoritative inventory. Differences between systems are investigated. A laptop visible in RMM but absent from EDR may represent a security gap. A server in backup but missing from inventory may reveal an undocumented asset.

Inventory establishes the population against which future security coverage can be reconciled. This is why inventory is not a one-time scoping exercise. Chapter 23 showed how continuous readiness depends on repeatedly comparing the expected population with the systems that protect it.

24.7 Identify Every External Provider That Touches the Environment

Modern contractors rarely operate every security and technology function internally. Redwood may depend on Summit Ridge for managed IT, a SOC for monitoring, Microsoft for cloud services, a backup provider, secure file exchange, an application vendor, telecommunications providers, and specialized implementation firms. The organization needs to know which providers affect systems or information in scope.

The key question is functional: what does this provider actually do? Does it process, store, or transmit protected information? Does it administer systems that do? Does it provide a security function such as SIEM, endpoint management, backup, or vulnerability management? Does it hold privileged credentials? Does it retain logs or evidence?

Provider discovery prevents the responsibility matrix from becoming fiction. If the SSP says Redwood monitors security logs but a SOC actually performs the function, the documentation should reflect reality. If Summit Ridge administers the tenant, its privileged access and operational procedures matter.

24.8 Build the Responsibility Matrix Before Writing Generic Policies

The responsibility matrix translates architecture into ownership. For each significant security function, Redwood identifies who is accountable, who performs the activity, who approves important decisions, who monitors it, who supplies evidence, and who receives escalation.

A requirement can be implemented by Redwood, Summit Ridge, another external provider, or a combination. Shared responsibility does not mean vague responsibility. If Summit Ridge deploys patches but Redwood approves production downtime, both roles should be visible. If a SOC investigates alerts while Summit Ridge performs containment, the handoff should be explicit.

This matrix becomes one of the most important implementation artifacts because it influences service agreements, procedures, evidence, assessment interviews, and ongoing operations. It also exposes gaps before technology is purchased. A row with no clear performer is a design problem.

24.9 Perform the Gap Assessment Against Reality

A gap assessment compares the required security outcomes with the environment that actually exists. The team should resist the temptation to answer questions from policy documents alone. If a policy says multifactor authentication is required but administrators can still log in through an excluded path without MFA, the technical reality matters.

For each requirement or assessment objective, Redwood and its advisors determine what implementation exists, what evidence supports it, what is missing, and who owns remediation. Summit Ridge demonstrates managed technologies where its services implement part of the requirement. The contractor supplies business processes and internal evidence.

The gap assessment should produce actionable work rather than a red-and-green spreadsheet that nobody can execute. A useful gap identifies the missing condition, affected systems, intended solution, responsible party, dependencies, evidence needed, and verification method.

24.10 Do Not Confuse a Gap Assessment With an Assessment Result

A readiness consultant can help Redwood understand gaps, but that activity is not automatically the formal assessment required by a contract. Likewise, an MSP's internal review is not a C3PAO assessment merely because it uses similar questions. The roles must remain clear.

This distinction protects the contractor from false confidence. A consultant may say that an environment appears ready, but the organization still needs the assessment mechanism applicable to its situation. Conversely, a formal assessment should not be the first time Redwood discovers how its own environment works.

The readiness phase exists to make the implementation deliberate and evidence-based before the organization reaches the formal assessment process.

24.11 Build the Target Architecture

After scope and gaps are understood, Redwood defines the environment it intends to operate. The target architecture describes identity, endpoints, networks, cloud services, applications, security monitoring, vulnerability management, backup, remote administration, collaboration, file transfer, and provider connections.

The architecture should answer why each major component exists. Identity establishes who is requesting access. MFA reduces the risk of password-only

compromise. Device management applies and verifies endpoint policy. EDR provides endpoint detection and response. Vulnerability management identifies weaknesses. Logging and SIEM provide visibility. Backup supports recovery. RMM supports managed administration but also creates a powerful control plane that must itself be protected.

Technology selection follows architecture. If the team starts with products, it can end with overlapping tools that do not form a coherent operating system.

24.12 Decide Whether Microsoft Commercial, GCC, or GCC High Fits the Requirement

Microsoft 365 Government decisions deserve careful treatment because contractors frequently hear the phrase 'you need GCC High' before anyone has analyzed the contract, information, export-control considerations, service requirements, or eligibility. GCC and GCC High are cloud environments, not CMMC certificates and not ordinary software packages that make an organization compliant when purchased.

Redwood identifies contractual and regulatory needs first. It then evaluates Microsoft service commitments, eligibility, feature availability, integrations, endpoints, operational requirements, and the data it intends to place in the environment. Where GCC High is appropriate, the project should be treated as an architecture and migration program rather than a license swap.

The target design considers tenant creation, domains and DNS, Entra identity, administrative roles, MFA, Conditional Access, Exchange, Teams, SharePoint, OneDrive, Intune, Defender or other security tooling, application integrations, logging, migration, endpoint enrollment, and ongoing administration. The team verifies current Microsoft Government documentation because feature availability and endpoints can change.

24.13 Phase One Deliverable: The Readiness and Compliance Design Package

At the end of Phase One, Redwood should possess enough understanding to explain what it is building and why. The package includes the contractual and information assumptions, preliminary scope, information-flow diagrams, asset and provider inventories, responsibility model, gap register, target architecture, documentation plan, implementation backlog, evidence plan, and decisions that still require resolution.

This package is not valuable because it is large. It is valuable because Phase Two can now implement an intentional design. The implementation provider should not arrive and ask which users need MFA after the project has already begun. Those decisions should emerge from the design.

Management also receives cost and sequencing information. Some gaps can be corrected immediately. Others depend on migration, procurement, application compatibility, provider contracts, or business-process changes. The roadmap makes those dependencies visible.

24.14 Phase Two Begins: Technical Implementation Is Where Design Becomes Reality

Technical implementation converts the approved architecture into functioning systems. This phase may involve Summit Ridge, a specialized Microsoft Government implementation provider, internal Redwood administrators, security vendors, and application specialists. Each participant needs a defined scope.

The implementation sequence should respect dependencies. Identity and administrative security influence nearly everything else. Endpoint enrollment depends on identity and management design. Collaboration configuration depends on tenant and information-flow decisions. Logging depends on knowing which systems are authoritative. Backup depends on knowing what must be recoverable.

Implementation should create evidence as it proceeds. Configuration records, change tickets, test results, migration records, screenshots where useful, exports, diagrams, and acceptance results become part of the evidence package rather than being reconstructed months later.

24.15 Identity First: Establish the Administrative Foundation

Before migrating business data, Redwood establishes administrative identities and privileged-role design. Administrative work should be attributable to individual identities wherever practical. Privileged access should be separated from ordinary user activity according to the architecture, protected with strong authentication, and limited to necessary roles.

Summit Ridge should not simply place every senior technician into permanent broad administrative roles. The MSP determines which technicians support Redwood, what roles they require, how emergency access works, how access is reviewed, and how technician departure removes customer access.

The implementation team tests both successful and denied access. A control is not proven merely because an administrator can log in. The team should demonstrate that an unauthorized or insufficiently privileged identity cannot perform the protected action.

24.16 MFA and Conditional Access: Implement the Access Policy the Business Designed

MFA adds another authentication factor so that a stolen password alone is less likely to provide access. Conditional Access can apply policy based on identity, device, application, location signals, risk, and other supported conditions. The important implementation question is what access model Redwood intends to enforce.

The team inventories exclusions because exclusions frequently become hidden weaknesses. Service identities, emergency accounts, legacy applications, and migration tools may require special treatment. Every exception should have a reason, owner, and lifecycle.

Testing includes normal users, administrators, managed devices, unmanaged devices where relevant, remote access, and exception cases. The implementation evidence records the policy and the test outcomes.

24.17 Endpoint Build: A Laptop Is Not Ready Because Windows Starts

Redwood defines a controlled endpoint build. A new laptop is entered into inventory, assigned to an authorized user, enrolled in device management, encrypted, protected by EDR, placed under RMM if that is part of the service, included in vulnerability and patch processes, configured with approved software, and validated before it receives access to protected workflows.

Summit Ridge can automate much of this process, but automation must be verified. A deployment script can fail. A device can appear in Intune but not EDR. A vulnerability agent can install but never register. The implementation team reconciles the same device across the relevant management systems.

The acceptance test deliberately creates a new test endpoint and follows the lifecycle from unboxed hardware to authorized production state. If the process depends on an engineer remembering seven separate consoles, the implementation has revealed an operational weakness before handoff.

24.18 EDR, RMM, Vulnerability Management, and Patching Must Be Designed as Different Functions

Beginners often assume one endpoint product performs every security function. EDR focuses on endpoint detection and response. RMM provides management and remote administration. Vulnerability management identifies weaknesses and exposure. Patch management deploys updates and tracks success and failure. Products can overlap, but the functions remain conceptually different.

Redwood and Summit Ridge define which platform is authoritative for each function and how exceptions flow into service management. If vulnerability scanning finds a critical issue, who creates the remediation task? If patching fails, who investigates? If EDR disappears from a device, who notices? If RMM can execute scripts across the environment, how is that administrative power protected?

Implementation succeeds when the tools form a workflow, not merely when all agents appear installed.

24.19 Network Architecture and Segmentation

The network design controls paths between users, systems, providers, and external networks. Redwood documents relevant segments, firewalls, remote access, wireless networks, administrative paths, and connections to cloud or provider services.

Segmentation can reduce exposure and scope, but only when the boundary is technically enforced and operationally respected. A VLAN label does not create meaningful isolation by itself. Firewall policy, routing, identity, administrative controls, and information-transfer procedures determine whether the separation is real.

The implementation team tests allowed and denied paths. It confirms logging for important network controls and records baseline configurations. Future drift can then be compared with the accepted design.

24.20 Logging, SIEM, and SOC Integration

Logging exists so the organization can understand important security and administrative events. A SIEM can aggregate and correlate records, while a SOC can monitor, investigate, and escalate according to its service. None of these components is valuable if the expected sources are unknown.

Redwood and Summit Ridge define which systems should produce security-relevant logs, where those logs go, how long they are retained as required by the design, and

who monitors them. If a SOC is used, the responsibility matrix identifies which alerts the SOC investigates and what happens when action is required.

Implementation includes source-health testing. The team intentionally verifies that the SIEM notices or operational staff can identify when an expected source stops reporting. Silence should not automatically be interpreted as safety.

24.21 Backup and Recovery: Design for the Business Service, Not Just the Server

Redwood identifies what must be recoverable and the business consequence of loss. Summit Ridge maps those needs to backup technology, retention, protection, and restoration procedures.

A server backup can be technically successful while the application remains unrecoverable because a database, license service, encryption key, identity dependency, or configuration was omitted. Recovery design therefore documents dependencies and restoration order.

Before handoff, the implementation team performs restoration tests. The test should demonstrate a meaningful recovery outcome, not merely that a backup file exists.

24.22 Secure Collaboration and File Exchange

Protected information needs approved paths for collaboration and transfer. Redwood defines how employees exchange files internally, with customers, and with subcontractors. The architecture may use appropriately configured Microsoft services, secure file exchange, customer portals, or other approved mechanisms depending on requirements.

The implementation should make the approved method usable. If the secure process is so cumbersome that engineers routinely bypass it, the architecture is fighting the business instead of protecting it.

Testing follows a representative file from authorized sender to authorized recipient, verifies access controls, examines audit evidence, and demonstrates removal of access when the relationship ends.

24.23 Application Compatibility and the Hidden Cost of Migration

A government-cloud or security migration can fail when the team focuses on Microsoft services but ignores the applications that employees actually use. CAD tools, ERP systems, scanners, multifunction devices, email relays, mobile

applications, APIs, scripts, plugins, and vendor portals may depend on authentication or endpoints that change.

Redwood inventories critical applications and integrations before cutover. Summit Ridge and specialized implementation providers test compatibility. Where an application cannot support the target environment, the team decides whether to replace it, isolate it, redesign the workflow, or seek another approved solution.

Unresolved incompatibilities should remain visible. Hiding them until migration weekend converts a design issue into an outage.

24.24 Migration: Move Identities and Information Without Losing the Security Story

Migration is not merely copying mailboxes and files. It changes where information resides, how users authenticate, which applications connect, which administrators have access, and where evidence is generated.

The migration plan identifies source and destination, sequencing, temporary accounts, coexistence periods, data validation, rollback considerations, user communication, and post-migration security checks. Temporary privileges and exceptions receive expiration points.

After migration, the team confirms that protected information is in the intended environment, access works only as designed, old access paths are closed, integrations function, security telemetry is present, and documentation reflects the new state.

24.25 Phase Three: Why Implementation Cannot End at 'It Works'

Many technology projects end when users can sign in and applications open. A CMMC-oriented security implementation needs another phase because somebody must operate the environment tomorrow. Phase Three is validation, knowledge transfer, and operational handoff.

The implementation provider demonstrates the environment against the design. Redwood and Summit Ridge receive architecture information, administrative procedures, known exceptions, migration history, diagrams, credentials through approved mechanisms, integration details, recovery information, and unresolved work.

The people accepting the system should perform tasks themselves. Watching the consultant click through a portal is not the same as demonstrating operational competence.

24.26 The Operational Acceptance Test

The Operational Acceptance Test, or OAT, asks whether the receiving organization can operate the security environment without depending on the implementation team's memory. Redwood and Summit Ridge select realistic tasks and execute them under observation.

The test begins with a new user. The administrator creates or provisions the identity according to the approved process, assigns the correct licensing and groups, verifies MFA enrollment, applies appropriate access, and confirms that unauthorized resources remain unavailable. The record shows authorization and resulting access.

Next comes a new endpoint. The team enrolls a test device, confirms management, encryption, EDR, RMM where applicable, vulnerability coverage, patch state, and access policy. It then demonstrates where a missing-agent condition would appear and how it becomes a ticket.

The team locates security logs, retrieves evidence, reviews an administrative change, handles a simulated Beacon escalation, isolates a test endpoint under the approved procedure, restores it to service, and documents the incident. It demonstrates a backup restore and traces an exception through approval and review.

Finally, the administrator disables the test user, revokes relevant access, retires the test endpoint, and shows that the lifecycle closes. If the receiving team cannot perform these operations, handoff is not complete.

24.27 What Must Be in the Handoff Package?

The handoff package should allow a qualified administrator to understand and maintain the environment. It includes the tenant and network architecture, administrative identities and roles, domains and DNS, licensing, Entra configuration, MFA and Conditional Access design, Exchange, Teams, SharePoint, OneDrive, Intune, endpoint-security configuration, RMM, vulnerability management, backup, logging, SIEM integration, device enrollment, applications, APIs, integrations, migration records, known exceptions, recovery information, diagrams, procedures, and unresolved issues.

The package should also identify where authoritative configuration lives. A PDF screenshot is useful evidence but should not be the only way the administrator knows how the tenant is configured. Operational documentation points to the live system and explains the intended state.

Ownership of each artifact is assigned. Documentation that nobody is responsible for maintaining begins decaying immediately.

24.28 Implementation Is Not Maintenance

The implementation provider may have exceptional knowledge of the migration but may not be contracted to operate Redwood's environment for the next three years. Summit Ridge may inherit ongoing administration. Redwood may retain some functions internally. Those roles must be distinguished before the project ends.

Maintenance includes user lifecycle, privileged-role review, endpoint onboarding, patching, vulnerability remediation, backup monitoring and testing, security-alert response, cloud-service changes, configuration drift, application approval, evidence retrieval, provider management, and documentation updates.

If the handoff assumes that 'the MSP will take care of it' without defining which MSP service covers each function, the implementation has transferred ambiguity rather than responsibility.

24.29 The Contractor Roadmap From Day One to Operational Readiness

Redwood's roadmap begins with contracts and information, moves into scope and ownership, then gap assessment and target design. It implements the technical and procedural controls, validates them, completes the applicable assessment and reporting activities, and transitions into continuous readiness.

Management remains involved at decision points: scope, business workflow, provider selection, risk and exceptions, downtime, information sharing, contractual interpretation, and affirmation where applicable. The contractor cannot outsource those decisions merely because Summit Ridge has stronger technical expertise.

The successful end state is not a folder labeled CMMC. It is a business environment in which protected work can be performed through known systems, by authorized people, using maintained security controls that produce evidence.

24.30 The MSP Roadmap From General IT Provider to CMMC-Capable Service Provider

Summit Ridge begins by examining its own services. Which technicians can access customer environments? How is RMM protected? How are credentials stored? How are customers separated? Which endpoint, vulnerability, backup, logging, ticketing,

and documentation platforms are used? Which external providers participate? What evidence can the MSP produce?

The MSP then maps its services to customer responsibilities without claiming that its product bundle equals CMMC compliance. It creates customer-specific security profiles, responsibility matrices, onboarding standards, escalation models, evidence procedures, and technician training.

Technicians learn the reason behind the controls. They know that a missing EDR agent is not simply a device-management problem; it creates a visibility gap. They know that an emergency firewall rule needs a lifecycle. They know that customer-specific authorization matters even when the same RMM console manages many organizations.

The MSP's end state is repeatable controlled service with room for customer-specific requirements. Standardization makes quality scalable; customer overlays prevent standardization from erasing contractual reality.

24.31 What Should the MSP Refuse to Promise?

Summit Ridge should not promise that buying its security bundle makes Redwood CMMC compliant. A technology stack can support requirements, but compliance depends on the contractor's complete environment, people, processes, contracts, information flows, providers, and evidence.

The MSP should also avoid claiming ownership of decisions it cannot make. It cannot determine business authorization for CUI access, decide contractual flowdowns on the contractor's behalf, or affirm facts it does not control. It can provide technical facts and evidence that support those decisions.

Clear boundaries strengthen the relationship. Redwood knows what it must own, and Summit Ridge can be held accountable for the services it actually performs.

24.32 The First 30 Days

In the first month, the project should emphasize discovery and control of immediate risk. Redwood establishes leadership, collects contract information, identifies FCI and CUI workflows, inventories systems and providers, and stops obviously uncontrolled practices where practical. Summit Ridge supplies technical inventories and explains the current environment.

The team begins the responsibility matrix and gap assessment. High-risk weaknesses such as unmanaged privileged access, missing MFA, unsupported exposed systems,

unknown remote-access paths, or unprotected endpoints receive early attention rather than waiting for a perfect master plan.

At the end of thirty days, management should understand the problem well enough to fund and sequence the next stage. The company may not be ready for assessment, but it should no longer be guessing about what the program contains.

24.33 Days 31 Through 60

The second month turns discovery into design and implementation. Scope assumptions are refined. The target architecture is approved. Technology and provider decisions are made. Policies and procedures are written to describe the intended operating model rather than copied from generic templates.

Identity, privileged access, endpoint standards, logging, vulnerability management, backup, and collaboration workflows begin moving toward the target state. Evidence collection starts immediately.

Where migration is required, application compatibility and user workflow receive serious attention. Training and communications prepare employees for changes in authentication, file handling, remote access, and approved collaboration.

24.34 Days 61 Through 90 and Beyond

The third month emphasizes completion, reconciliation, testing, documentation, and handoff. The team compares expected assets with security-platform coverage, closes implementation gaps, tests recovery, validates monitoring, exercises incident escalation, reviews privileges, and completes representative user and device lifecycles.

The SSP and related documentation are updated to describe the implemented environment. Evidence is organized by the claims it supports. Remaining gaps are handled according to the current rules applicable to the organization's level and assessment path; the team does not assume that every unmet requirement can simply be placed on a POA&M.

Operational Acceptance Testing demonstrates that Redwood and Summit Ridge can maintain the environment. The project then transitions from implementation cadence into the daily, weekly, monthly, quarterly, annual, and event-driven continuous-readiness rhythm developed in Chapter 23.

24.35 A Failure Scenario: Redwood Buys the Tools Before Doing the Design

Imagine Redwood skips Phase One. A reseller recommends EDR, SIEM, vulnerability scanning, a government-cloud migration, and a compliance platform. Management approves the purchase because the bundle sounds comprehensive.

Three months later, the tools exist but responsibility is unclear. The SIEM receives logs from only part of the environment. The vulnerability scanner cannot reach an engineering segment. The backup provider protects servers but not a cloud application the business assumes is covered. GCC High was purchased for some users while a legacy workflow still sends CUI through another system. The compliance platform shows many green controls because policies were uploaded.

The failure was not lack of spending. It was lack of architecture. Redwood must now perform the discovery and design work it skipped, often while paying for tools that may need to be reconfigured or replaced.

24.36 A Failure Scenario: The Consultant Leaves Without Operational Handoff

A specialized implementation provider completes a Microsoft Government migration. Users can sign in, mail flows, and the project is declared successful. Two weeks later, Summit Ridge receives an alert involving Conditional Access and discovers that nobody documented several migration exclusions or the service account used by an integration.

The consultant knew why the exceptions existed, but that knowledge left with the project team. Summit Ridge is afraid to remove them because doing so may break production. Redwood now has technical debt created by incomplete handoff.

Phase Three would have exposed the problem. Operational Acceptance Testing would have required Summit Ridge to explain the access model, exceptions, integrations, and evidence. The handoff package would have recorded owners and expiration conditions.

24.37 A Failure Scenario: The MSP Assumes the Contractor Owns Everything 'Compliance'

Summit Ridge tells Redwood that compliance is the customer's responsibility and therefore refuses to explain how its own services operate. The statement contains a partial truth but produces the wrong operating result. Redwood remains accountable

for its obligations, yet it cannot document or demonstrate controls that depend on the MSP without information from the MSP.

A mature MSP distinguishes accountability from service responsibility. It supplies architecture descriptions, procedures, service boundaries, technician-access controls, patch and vulnerability records, backup evidence, incident records, and other information relevant to the services it performs.

Redwood combines that provider evidence with its own business and governance evidence. Shared implementation becomes demonstrable without pretending the MSP has become the contractor.

24.38 A Failure Scenario: The Contractor Assumes the MSP Owns Everything

The opposite failure occurs when Redwood tells Summit Ridge to 'make us CMMC compliant' and disengages. Summit Ridge can improve technology, but it cannot decide which employee should receive CUI, which subcontractor is authorized, what new contract changes scope, or whether a business exception is acceptable.

The gap becomes visible during implementation. Engineers use an unapproved transfer path because no business owner participated in workflow design. A new subcontractor is onboarded without security review because procurement never joined the program. Policies describe approvals that management has never performed.

The correction is governance. Redwood names accountable leaders, integrates contracting and business processes, and uses Summit Ridge as an operational partner rather than a substitute for organizational responsibility.

24.39 The Evidence Plan Starts on Day One

Evidence should not be an assessment-week project. During Phase One, Redwood identifies what kinds of evidence will demonstrate each important process and where those records will originate. During Phase Two, implementation records establish the initial state. During Phase Three, test results demonstrate operation. After handoff, normal service records demonstrate continuing effectiveness.

Summit Ridge configures its PSA and technical platforms so customer-specific records can be retrieved. Beacon or another SOC retains investigation and escalation records according to the service design. Redwood maintains approvals, training, policies, contracts, information-flow decisions, and management records.

The evidence library should preserve meaning. A screenshot without date, system, scope, or explanation can become difficult to interpret. A ticket connected to the affected asset, authorization, action, and verification tells a stronger operational story.

24.40 How to Know When You Are Ready for Readiness Validation

Redwood is ready for deeper validation when the implemented environment is stable enough to test honestly. The organization can explain scope, identify assets and providers, demonstrate responsibility, show technical configurations, produce evidence, and perform representative operational workflows.

Validation should deliberately look for failure. Select a new laptop and trace enrollment. Select a terminated employee and trace access removal. Select a vulnerability and trace remediation. Select a backup and restore it. Select a firewall change and trace approval. Ask the SOC to demonstrate source health. Ask Summit Ridge to retrieve evidence without advance staging.

Every failure becomes an improvement item. The objective is not to produce a perfect rehearsal score. It is to discover where the operating model breaks while the organization still controls the schedule.

24.41 Preparing for the Applicable Assessment Path

The assessment path depends on the current contractual and regulatory situation. As of September 2026, DoD states that CMMC implementation is paused in Phase I and describes Level 1 annual self-assessment and Level 2 self-assessment every three years with annual affirmation under the current Phase I posture. Current DFARS and 32 CFR requirements should be checked for the contract and date at issue.

Regardless of assessment mechanism, Redwood should prepare by validating scope, evidence, participants, system access, demonstrations, and consistency between documents and reality. People should understand their own responsibilities rather than memorize scripted answers.

Summit Ridge and other providers prepare to support questions about the services they perform. They should know which evidence they can supply and which questions belong to Redwood.

24.42 Transition to Continuous Readiness

After the applicable assessment or readiness milestone, Redwood does not dissolve the project and wait for the next cycle. The implementation backlog becomes an

operational backlog. Responsibility moves from project teams to permanent owners. Evidence continues through ordinary work.

Chapter 23's operating rhythm now becomes active: daily exception handling, weekly backlog review, monthly coverage and service review, quarterly governance and privileged-access review, annual program validation, and immediate review when significant business or technical events occur.

The handoff from Chapter 24 to Chapter 23 is deliberate. A program built correctly from Day One is designed to be maintainable. Continuous readiness is not an extra layer added later.

24.43 The Contractor and MSP Side by Side

Redwood knows the contract, business purpose, authorized users, information, subcontractors, and acceptable business risk. Summit Ridge knows the managed infrastructure, service platforms, technical configuration, operational workflows, and technician procedures. Beacon knows monitoring and investigation. Cloud and technology providers operate their assigned services.

The program works when those perspectives are connected. A new contract changes the information flow; Redwood triggers review. The review identifies a new server and collaboration requirement; Summit Ridge implements the controls. Beacon receives the new log source. The responsibility matrix and SSP are updated. Evidence is produced. Continuous monitoring confirms operation.

No participant owns the entire story, but the contractor must be able to understand and govern the complete story.

24.44 A Complete Day-One-to-Operations Walkthrough

Redwood receives a defense opportunity that will involve CUI. Contracting identifies the applicable requirements and alerts management. The security lead convenes engineering and Summit Ridge. They trace the expected CUI flow and discover that the existing commercial collaboration process is not the intended future architecture.

The team scopes the proposed environment, inventories assets and providers, performs the gap assessment, and assigns responsibilities. It chooses an architecture appropriate to the actual contractual and technical requirements. Microsoft Government services are evaluated rather than assumed. Endpoint, identity, network, logging, vulnerability, backup, and collaboration controls are designed as an integrated system.

Phase Two implements the environment. Identities and privileged roles are established. Endpoints are enrolled and reconciled. Network paths are controlled and tested. Logging reaches the monitoring function. Backups are configured and restored. Applications and integrations are validated. CUI workflows are tested end to end.

Phase Three forces the receiving team to operate what was built. Summit Ridge provisions and removes a test user, enrolls and retires a test endpoint, investigates a missing agent, retrieves evidence, responds to a simulated SOC escalation, verifies a restore, and explains significant exceptions. Redwood validates business authorization, information handling, provider responsibilities, and documentation.

The applicable assessment and reporting process is completed according to current requirements. Then ordinary Monday arrives. An EDR agent stops reporting. The program does not panic and it does not wait for an assessor. Monitoring identifies the exception, Summit Ridge investigates, the endpoint is corrected, the result is verified, and the ticket becomes evidence. That moment is the real completion of the Day-One journey: the organization has moved from building controls to operating them.

24.45 Questions Every Contractor Should Be Able to Answer Before Declaring the Program Operational

Redwood should be able to explain why CMMC requirements apply to the work it is performing, what protected information it receives or creates, where that information flows, which systems and people participate, which providers support the environment, and why the chosen architecture fits the business.

It should be able to identify who owns each major security function, how new users and devices enter the environment, how departed users leave it, how vulnerabilities become remediation work, how backups are tested, how incidents are escalated, how significant changes update documentation, and how evidence is retrieved.

Most importantly, Redwood should be able to explain what happens tomorrow when something changes. If the program only describes the environment that existed on implementation day, it is not operational.

24.46 Questions Every MSP Should Be Able to Answer Before Calling Its Service CMMC-Ready

Summit Ridge should be able to explain exactly which services it performs for Redwood and which it does not. It should identify technician access, RMM protections, credential management, customer separation, endpoint coverage,

vulnerability workflow, patch exceptions, backup operations, logging relationships, incident escalation, and evidence sources.

It should demonstrate how a new customer is onboarded, how customer-specific requirements modify the standard service, how technicians are trained, how a departing technician loses customer access, how tool migrations preserve coverage and evidence, and how the MSP detects failure in its own service platforms.

It should also be able to say where its authority stops. A CMMC-capable MSP is not one that promises to own everything. It is one that performs its assigned responsibilities consistently, transparently, securely, and evidentially.

24.47 Final Perspective: Build for the Tuesday After the Project Ends

The strongest CMMC implementation is not the one with the most impressive kickoff presentation or the largest technology purchase. It is the one that still works after the consultants leave, after employees change, after Microsoft changes a service, after a critical vulnerability appears, after the MSP changes a platform, and after management wins a new contract.

Day One begins with understanding. Phase One turns understanding into design. Phase Two turns design into functioning technology and processes. Phase Three proves that the receiving organization can operate what was built. Continuous readiness keeps the program aligned with reality.

The contractor cannot outsource accountability, but it can and often should rely on capable providers for assigned operational functions. The MSP cannot own the contractor's entire CMMC obligation, but its services can materially determine whether the contractor can protect information and demonstrate that protection.

The program is complete enough to operate when normal work creates security, normal work creates evidence, change enters controlled processes, failures become visible, responsibilities are understood, and the organization can explain the current environment without reconstructing it from memory. That is what it means to build a CMMC program from Day One.

Current Regulatory Note for This Edition

As reviewed in September 2026, the official DoD CMMC site states that Phase II requirements originally scheduled for November 10, 2026 were suspended on July 13, 2026 and that Phase I self-assessment requirements remain in place. The official page describes Level 1 annual self-assessment and annual affirmation and Level 2

self-assessment every three years with annual affirmation under the current Phase I posture.

Current DFARS 252.204-7021 defines current CMMC statuses and, when the clause applies, requires the contractor to have and maintain the required current CMMC status for covered information systems used in contract performance, complete annual affirmation of continuous compliance in SPRS for applicable CMMC UIDs, address applicable subcontractor requirements, and close a valid POA&M when operating under a Conditional status. Because CMMC implementation is currently under review and regulatory details can change, readers should verify the current DoD CIO, 32 CFR part 170, DFARS, contract, and solicitation before making implementation or contractual decisions.

Chapter 24 Deep Implementation Expansion: The Questions a Beginner Will Ask Next

The first portion of this chapter established the Day-One roadmap. This expansion deliberately slows the journey down. It answers the operational questions that appear after a reader understands the roadmap but still needs to know how to execute it, who makes each decision, what can fail, how the failure is detected, how it is corrected, how the correction is verified, and what evidence remains.

24.48 Who Should Lead the Program on Day One?

Redwood needs one internally accountable leader even if the company is too small to employ a full-time CISO or compliance department. The leader does not need to perform every technical task. The leader needs authority to bring contracting, engineering, management, HR, procurement, and Summit Ridge into the same program and to resolve ownership disputes.

The technical lead and the accountable business lead can be different people. Summit Ridge can serve as a technical partner, and a readiness specialist can advise on CMMC requirements, but neither should silently become Redwood's executive decision-maker. The contractor needs an internal person who can say which business processes are approved, which risks require management attention, and which contractual questions must be escalated.

A Day-One kickoff should therefore end with named roles, not merely a project calendar. Who owns the program? Who owns contracts? Who owns the technical environment? Who approves user access? Who can authorize downtime? Who handles incidents? Who maintains documentation? Who coordinates evidence? If the organization cannot answer those questions, implementation will repeatedly stall.

24.49 What Should the Day-One Kickoff Meeting Actually Cover?

The kickoff is a discovery meeting, not a sales presentation. Redwood explains what government work it performs or intends to perform, which contracts or solicitations drive the project, which locations and teams participate, and what protected information it expects. Summit Ridge explains the current technical environment and service boundaries.

The group identifies known unknowns. Does Redwood know where CUI enters? Are employees using personal devices? Are engineering files exchanged through commercial services? Does a subcontractor receive protected drawings? Does the existing backup provider touch systems in scope? Are administrators using shared

accounts? Unknown answers become assigned discovery tasks rather than assumptions.

The meeting should also establish communication and change discipline. While the program is being designed, Redwood should not introduce a new SaaS platform or major infrastructure change without telling the project team. Otherwise the target keeps moving while scope is being established.

The output is a working decision log, discovery backlog, ownership list, source-document list, and schedule for information-flow and technical workshops.

24.50 How Do We Read a Contract Without Turning the MSP Into a Lawyer?

Summit Ridge needs enough contractual context to understand technical requirements, but the MSP should not provide legal conclusions outside its role. Redwood's contracting personnel, counsel where appropriate, and qualified compliance resources determine what clauses and obligations apply.

The technical team asks operational questions. What information must be protected? What assessment level or status is required by the contract? Are there specific cloud, incident-reporting, export-control, subcontractor, or data-location requirements? Are there customer-specific security requirements beyond the baseline?

Those answers become technical design inputs. If the contract changes, Redwood notifies the security program. Summit Ridge then evaluates whether architecture or operations must change. This keeps contract interpretation with the contractor while ensuring that contractual decisions actually reach the people configuring systems.

24.51 How Do We Discover CUI When Employees Do Not Know What to Call It?

Employees may understand the work without understanding CUI terminology. An engineer may say, 'the customer sends us drawings,' while a program manager says, 'we receive technical data through the portal.' Discovery interviews should therefore focus on business activity before demanding that every employee classify information.

The interviewer asks what the employee receives, from whom, through which system, where it is saved, which application opens it, who else uses it, whether it is printed, whether it is copied into reports, whether it is sent to suppliers, and how it is archived. Markings and contractual guidance are then examined with the appropriate business and compliance personnel.

This method often discovers secondary copies. A drawing arrives through an approved portal but is exported to a desktop folder, attached to a ticket, synchronized to a collaboration site, included in backup, and copied into an engineering package. The original portal was only the beginning of the flow.

The evidence of discovery is the resulting information-flow record and the decisions made from it, not a claim that every employee became a classification expert overnight.

24.52 How Do We Decide What Is In Scope Without Guessing?

Scoping should follow current CMMC scoping guidance and the actual architecture. Redwood identifies assets that process, store, or transmit relevant information and then evaluates supporting security and specialized assets according to the applicable guidance. External services are included in the analysis where their functions affect the environment.

The team should document the reason for boundary decisions. If a corporate HR system is considered outside the CUI environment, what prevents CUI from entering it? If an engineering enclave is segmented, what controls the boundary? If Summit Ridge's RMM administers in-scope endpoints, how is that provider relationship documented?

Uncertainty should be visible. A questionable system can remain an open scoping decision while authoritative guidance is obtained. Quietly excluding it because inclusion would be inconvenient is not a defensible method.

Scope is then revisited after implementation. The final architecture may differ from the initial design, and the documented boundary must describe what was actually built.

24.53 How Do We Decide Between Enterprise-Wide Protection and an Enclave?

An enterprise-wide approach applies the security architecture broadly. It can simplify user workflow because employees do not constantly cross a special boundary, but it may increase the population of systems, users, applications, and providers that must be controlled and evidenced.

An enclave concentrates protected work in a more limited environment. That can reduce scope, but it creates boundary-management challenges. Users must know where protected work is permitted. Data transfer into and out of the enclave must be

controlled. Applications needed by engineering must work inside the environment. Remote support and administrative tools must be designed around the boundary.

Redwood should model real employee tasks before deciding. If an engineer needs ten applications and constant collaboration with colleagues outside the enclave, a theoretically narrow design may create daily pressure to bypass controls. If only a small team handles CUI through a stable workflow, segmentation may be practical.

The correct architecture is the one Redwood can operate securely for years, not the one that creates the smallest diagram for assessment week.

24.54 How Do We Build an Inventory When Our Existing Lists Disagree?

Disagreement is normal. RMM may show 143 devices, EDR 139, Intune 136, vulnerability management 141, and the accounting asset list 150. The project should not choose whichever number looks best. It should reconcile the differences.

Each unexplained device becomes a question. Is it retired? Offline? A server without Intune? A newly purchased laptop? A stale EDR record? An unmanaged machine? A virtual system? Reconciliation creates the authoritative population and exposes control gaps at the same time.

The inventory should identify enough attributes to support security operations: unique identifier, hostname, owner or custodian, device type, location or logical environment, operating system, management status, relevant information category, and lifecycle state. Additional fields can be added where useful.

After implementation, the reconciliation process continues. The initial inventory is valuable because it becomes the baseline against which future additions and retirements are recognized.

24.55 How Do We Inventory Software and Integrations?

Hardware inventory alone cannot reveal the complete environment. Redwood identifies major applications, SaaS services, browser extensions where relevant, scripts, APIs, service accounts, email relays, engineering plugins, and integrations that participate in protected workflows or security operations.

Summit Ridge can use endpoint discovery and cloud administration data, but interviews remain important. An engineering team may use a specialized vendor portal that never appears as installed software. An accountant may have authorized an OAuth application directly in Microsoft 365.

For each important integration, the team asks what identity it uses, what data it can access, where credentials are stored, what endpoint it connects to, who owns it, how it is monitored, and what happens if it fails.

This becomes especially important during GCC or GCC High migration because an integration that works in a commercial cloud may require different endpoints, capabilities, or vendor support in a government environment.

24.56 How Do We Evaluate an External Service Provider?

Redwood first defines what the provider will do. A provider that merely sells hardware creates a different risk from a provider that remotely administers CUI systems or stores backups. Function determines the depth of review.

The team evaluates access, information handling, service boundaries, security responsibilities, incident communication, personnel access where relevant, logging and evidence, subcontracted dependencies, continuity, and termination procedures. Contractual requirements applicable to the relationship are reviewed by Redwood.

Summit Ridge should participate when the provider integrates technically with systems it manages. It can identify required ports, APIs, identities, administrative access, log sources, and operational dependencies.

The provider decision and responsibility should be documented before production use. A vendor questionnaire by itself is not the architecture; it is one input into the decision.

24.57 How Do We Turn a Gap Into an Implementable Work Item?

A weak gap says, 'MFA missing.' A useful implementation item identifies where MFA is missing, which identities and access paths are affected, the intended control, dependencies, owner, business impact, test method, and evidence.

For example, Redwood may discover that standard Microsoft 365 users use MFA but a legacy VPN authenticates with username and password only. The remediation is not 'turn on MFA everywhere.' The team determines whether the VPN supports the intended identity provider, whether replacement is needed, which users depend on it, how emergency access works, and how the new flow will be tested.

Summit Ridge creates technical tasks. Redwood owns business decisions such as outage timing or replacement funding. The readiness lead tracks the gap until implementation and verification are complete.

This approach prevents the project from reaching the end with dozens of items marked 'in progress' that nobody can translate into concrete work.

24.58 How Do We Prioritize Gaps?

Priority combines security consequence, contractual significance, dependency, exploitability, business impact, and implementation sequencing. A missing privileged-access control may deserve immediate attention even if another gap is easier to close.

Dependencies matter. Redwood cannot fully validate endpoint Conditional Access until device enrollment is functioning. Logging design may depend on final architecture. Migration may depend on application compatibility. The roadmap should therefore distinguish risk priority from project sequence.

Quick wins are useful when they reduce real risk, but the program should not spend its first month closing cosmetic documentation gaps while privileged accounts remain uncontrolled.

Management receives a roadmap that explains why the order exists. This makes funding and schedule decisions understandable rather than arbitrary.

24.59 How Do We Write Policies That Describe Reality?

Policy should establish organizational expectations and authority. Procedure explains how people perform the work. Technical configuration implements portions of those expectations. Evidence demonstrates that the work and configuration exist.

Redwood should avoid copying a large policy set and changing the company name. A copied policy may require a committee the company does not have, reference technology it does not use, or promise review frequencies nobody performs.

The team writes policy around the intended operating model, then validates it against implementation. If policy says privileged access is reviewed quarterly, the organization must assign the reviewer, define the population, schedule the review, retain the record, and handle discovered excess access.

A policy becomes credible when ordinary operations can demonstrate it.

24.60 How Do We Build the SSP While the Environment Is Still Changing?

The SSP can begin during design as a controlled working document. Early sections describe the organization, scope assumptions, environment, and intended

implementations. As Phase Two progresses, intended language is replaced or refined to describe the implemented state.

Redwood should clearly distinguish planned controls from operating controls during the project. Otherwise a draft SSP can create false confidence by describing technology that has not yet been deployed.

Summit Ridge and other providers supply accurate descriptions of the services they perform. Redwood integrates those descriptions into the complete system story and identifies provider responsibilities.

Before readiness validation, the SSP is compared with the live environment. The final document should explain what exists, not what the project originally hoped to build.

24.61 How Do We Choose Technology Without Believing the Vendor's Compliance Label?

Vendors often market products as CMMC-ready, CMMC-compliant, government-ready, or designed for regulated environments. Those descriptions can identify useful capabilities, but Redwood still has to determine whether the product fits its architecture and requirements.

The evaluation starts with function. What security problem are we solving? What capability is required? How will the product integrate? Who will operate it? What evidence will it produce? What happens when it fails? Does it support the cloud environment and endpoints we actually use?

Then the team evaluates provider commitments, technical features, administration, logging, retention, APIs, support, licensing, government-cloud compatibility where needed, and lifecycle cost. Summit Ridge evaluates operational fit because a product the MSP cannot reliably maintain may become a long-term weakness.

Product selection ends with an implementation and ownership plan, not a purchase order.

24.62 How Do We Protect the RMM Platform That Can Control Everything?

RMM is powerful because it allows Summit Ridge to administer many Redwood systems remotely. The same capability creates concentrated risk. A compromised RMM identity or automation function can provide broad control over customer endpoints.

Summit Ridge therefore protects RMM with strong authentication, least privilege, individual technician identities, customer separation, logging, role design, restricted automation, access review, and secure administrative practices appropriate to the platform and risk.

The MSP should know which technicians can access Redwood and why. A technician leaving Summit Ridge triggers removal across the RMM and any customer-specific systems. High-risk scripts and mass actions deserve additional control because an error can affect many systems at once.

Redwood should understand the RMM's role in its environment even if it does not administer the platform. The service is part of the security architecture because it provides privileged remote administration.

24.63 How Do We Build an Evidence Map?

For every important control or process, Redwood asks what claim it needs to demonstrate and which record best supports that claim. If the claim is that only authorized users receive access, evidence can include authorization, identity configuration, access reviews, and lifecycle records.

The map identifies the system of record, evidence owner, retention consideration, retrieval method, and whether the evidence shows current state, repeated operation, or a specific event.

Summit Ridge maps technical evidence from PSA, RMM, EDR, vulnerability management, patching, backup, and administrative logs. Beacon maps monitoring and incident evidence. Redwood maps business authorization, policies, training, contracts, and governance.

The evidence map exposes dependencies early. If an important record will disappear after thirty days because of licensing, the organization can address retention before an assessment needs older evidence.

24.64 How Do We Design User Onboarding From the Beginning?

User onboarding starts with business authorization. Redwood identifies the employee, role, projects, information needs, and required applications. Summit Ridge provisions the identity and technical access according to that authorization.

The process should avoid broad default access. Groups and roles are mapped to job needs. MFA enrollment, device issuance, required training, approved software, remote access, and project-specific permissions are completed before protected work begins.

Verification is important. The team tests that the user can reach authorized resources and cannot reach representative unauthorized resources. Problems are corrected before the workflow becomes normal.

The onboarding record becomes evidence of authorization, provisioning, and validation.

24.65 How Do We Design Offboarding Before the First Person Leaves?

Offboarding should be designed during implementation because waiting for a real termination is too late to discover that access exists in six independent systems. Redwood and Summit Ridge inventory identity dependencies and define the termination trigger.

The workflow addresses central identity, sessions, MFA methods, VPN, RMM or administrative access where applicable, SaaS applications, privileged roles, guest relationships, direct application accounts, devices, shared secrets, and physical access where relevant.

A test user can be terminated during Operational Acceptance Testing. The team searches for residual access afterward. Any account that survives reveals a missing dependency.

This turns offboarding from an HR email into a tested security process.

24.66 How Do We Handle Service Accounts and APIs?

Service identities and API credentials can become invisible because they do not correspond to employees who appear in HR reports. Redwood and Summit Ridge inventory them separately, identify owners, purpose, permissions, credential storage, rotation or lifecycle, and dependencies.

Where modern managed identities or stronger authentication methods are available and appropriate, the architecture can reduce reliance on static secrets. Where secrets remain necessary, they should be protected and access controlled.

During migration, service accounts deserve special testing. A human user may authenticate successfully while an automated integration silently fails because its endpoint or authentication method changed.

Operational handoff must identify these identities so the receiving team does not discover them only after an expired credential causes an outage.

24.67 How Do We Implement Logging Without Collecting Everything Forever?

Logging design starts with security and operational questions rather than unlimited collection. Which events are needed to detect misuse, investigate incidents, verify administrative changes, and support evidence? Which systems are authoritative? How quickly must events be available?

Redwood and its providers balance visibility, retention, cost, and sensitivity. More logs are not automatically more useful if nobody can interpret them. Critical identity, endpoint, network, cloud, and administrative sources receive deliberate attention.

Beacon or another monitoring provider defines what it actively monitors versus what is merely retained. That distinction belongs in the responsibility model.

Testing includes both event generation and source failure. The team confirms that a representative event appears and that loss of an expected source can be recognized.

24.68 How Do We Build Vulnerability Management From Zero?

Redwood first establishes the asset population to be assessed. Summit Ridge deploys or configures the chosen vulnerability capability and verifies coverage. Initial scans often produce a large backlog, so the team needs a triage and remediation model.

Findings are prioritized using severity and context. Ownership is assigned. Patches, configuration changes, mitigations, upgrades, or replacement may be required. Business-impact decisions go to Redwood.

After remediation, the team verifies that the vulnerable condition is gone. A closed ticket without technical verification is incomplete.

The initial backlog becomes a useful measure of progress, but the permanent process matters more. New vulnerabilities will continue appearing after the project ends.

24.69 How Do We Build Patch Management From Zero?

Patch management begins by identifying operating systems, applications, firmware, and devices that require updates. Redwood and Summit Ridge establish maintenance windows, emergency procedures, testing needs, reboot expectations, and exception authority.

The implementation team should test the failure path. What happens when a device misses the window? When an update fails? When an engineering application cannot

support the latest patch? Those cases become queues with owners rather than invisible leftovers.

Reporting focuses on exceptions and age, not merely a high success percentage. The remaining unpatched systems receive context and disposition.

Patch evidence includes deployment records, failure investigation, exceptions, and verification.

24.70 How Do We Build Backup and Recovery From Zero?

Redwood identifies business services and data that require recovery, then defines realistic recovery expectations. Summit Ridge maps systems and dependencies to backup technology.

The team verifies coverage against inventory so a newly discovered server is not silently omitted. It protects backup administration and credentials because attackers often target recovery systems.

Restoration tests begin during implementation. A file restore proves one capability; an application recovery proves more. The team documents dependencies and improves the runbook after failures.

Operational handoff assigns responsibility for daily failures, periodic tests, capacity, retention, new-system enrollment, and evidence.

24.71 How Do We Build Incident Response Before We Have Had an Incident?

Redwood defines what constitutes an incident, who coordinates response, how employees report suspicious activity, how Beacon or another SOC escalates, what Summit Ridge may do, and when management becomes involved.

The plan identifies after-hours contacts and pre-authorized containment actions. It distinguishes routine security alerts from events requiring management, legal, contractual, or reporting analysis.

Tabletop exercises test the plan. A simulated compromised workstation asks whether Beacon can reach Summit Ridge, whether Summit Ridge can isolate the endpoint, whether Redwood knows who decides about business shutdown, and whether evidence can be preserved.

Lessons from the exercise become implementation tasks before a real attacker tests the process.

24.72 How Do We Train Employees Without Turning Training Into an Annual Video?

Employees need general security awareness, but they also need workflow-specific understanding. Redwood engineers should know where CUI is allowed, which transfer method to use, what to do when a customer sends information through an unexpected path, and how to report a mistake quickly.

Administrators need deeper role-based training because their actions can change security controls. Summit Ridge technicians supporting Redwood need customer-specific context, escalation rules, approved tools, and evidence expectations.

Training should connect to real scenarios. An employee who understands why copying a drawing into an unapproved AI service changes the information flow is better prepared than one who merely remembers a quiz answer.

Training records provide evidence, but changed behavior is the actual objective.

24.73 How Do We Handle AI Tools From Day One?

AI services can create new information flows very quickly. Redwood should decide which AI services are approved, what information may be entered, what business uses are permitted, and how employees request new capabilities.

The security review considers data handling, provider terms and commitments, authentication, retention, integrations, administrative controls, and whether protected information is involved. The exact decision depends on the service and contractual context.

Summit Ridge can help enforce technical restrictions where feasible, but policy and business authorization remain Redwood responsibilities.

The objective is not to ban innovation reflexively. It is to prevent employees from creating unreviewed external data flows simply because a tool is convenient.

24.74 How Do We Validate Microsoft Government Cloud Implementation?

Validation begins with the architecture and the current Microsoft documentation for the selected environment. The team confirms tenant and domain configuration, administrative roles, authentication, Conditional Access, collaboration settings, device management, endpoint-security integration, logging, applications, and relevant service configuration.

It tests representative users and devices rather than relying only on portal screenshots. Can an authorized managed device access the intended resource? What happens from an unmanaged device? Can an administrator perform the intended task? Does the action appear in audit records?

Integrations receive separate validation because national cloud endpoints and feature availability can differ from commercial environments. The team verifies the exact services it uses rather than assuming parity.

The final evidence records the implemented configuration and operational tests, while the handoff documentation explains how the receiving team maintains it.

24.75 How Do We Know GCC High Is Actually Necessary?

The decision should come from Redwood's contractual, regulatory, information, eligibility, and technical requirements, not from the statement that 'CMMC means GCC High.' CMMC and Microsoft cloud selection are related through the contractor's actual requirements, but they are not synonymous.

Redwood reviews the contract and data types, including any additional requirements such as export-controlled information where relevant. It examines Microsoft's current service descriptions and commitments for the candidate environment. Technical teams evaluate application and integration compatibility.

If GCC High is selected, the decision record explains why. If another environment is selected, the record explains why that architecture satisfies the applicable requirements. This makes the cloud decision defensible and maintainable.

Because Microsoft Government offerings and regulatory requirements can change, the decision should be revalidated when material contracts or architecture change.

24.76 What Happens During a Government-Cloud Migration Weekend?

Migration weekend should be the execution of a rehearsed plan, not the moment the team discovers dependencies. User waves, mailbox or data movement, DNS changes, authentication, devices, applications, support staffing, rollback criteria, and communications are prepared in advance.

Temporary administrative roles and migration accounts are tracked. Summit Ridge and the implementation provider monitor identity, mail flow, collaboration, endpoint enrollment, and critical integrations. Redwood provides business testers who can confirm real workflows.

After cutover, validation extends beyond 'email works.' Users test approved CUI workflows, security telemetry, Conditional Access, endpoint health, collaboration permissions, and evidence generation.

The project remains in heightened support until exceptions are understood and the environment is stable enough for handoff.

24.77 What Does Knowledge Transfer Actually Look Like?

Knowledge transfer is a series of operational demonstrations and guided exercises. The implementation provider explains architecture and then asks Summit Ridge or Redwood administrators to perform tasks. Questions and failures are expected.

The receiving team practices user lifecycle, device enrollment, policy troubleshooting, log retrieval, application administration, incident escalation, backup recovery, evidence retrieval, and change procedures. It learns where vendor documentation applies and where customer-specific configuration differs.

Sessions are recorded or documented where appropriate, but recordings do not replace usable procedures. The team converts recurring operations into concise runbooks with escalation paths.

Knowledge transfer is complete when the receiving team can operate the environment, not when the presenter reaches the last slide.

24.78 What Does a Failed Operational Acceptance Test Mean?

A failed OAT is useful. If Summit Ridge cannot enroll the test device without calling the implementation consultant, the handoff is incomplete. If a log cannot be found, evidence or monitoring design may be incomplete. If disabling the test user leaves an application account active, offboarding has a gap.

Each failure becomes a corrective item with an owner. The team fixes the process, documentation, configuration, or training and repeats the test.

Redwood should resist pressure to sign acceptance merely because the project schedule ended. Acceptance means the receiving organization can operate the agreed environment and understands unresolved exceptions.

The final OAT record can show initial failures and successful retests, demonstrating that validation actually challenged the implementation.

24.79 Who Owns the System After Handoff?

Ownership becomes distributed but explicit. Redwood owns the business system and its obligations. Summit Ridge owns the managed services assigned to it. Beacon owns its monitoring service. Microsoft and other providers own their service responsibilities. Internal administrators own the tasks retained by Redwood.

The responsibility matrix is updated from project language to operating language. A migration provider may disappear from most rows after handoff. Summit Ridge may become the performer for identity, endpoints, backup, and cloud administration. Redwood remains the approver for business access and significant risk decisions.

Support contacts, escalation, evidence ownership, and documentation ownership are confirmed before the project team disbands.

This is the bridge from Chapter 24 implementation into Chapter 23 continuous readiness.

24.80 What Happens on the First Monday After Handoff?

At 8:00 a.m., nobody opens the implementation project plan. Summit Ridge reviews operational exceptions. Beacon reviews security monitoring. Redwood begins normal protected work.

A test of the new operating model arrives quickly: one endpoint fails a management check-in. Summit Ridge's health monitoring creates an exception. The technician investigates, discovers a damaged agent after an update, repairs it, verifies EDR and vulnerability coverage, and closes the ticket with evidence.

Redwood did not need the implementation consultant. The security function detected degradation, assigned work, corrected it, verified the outcome, and preserved a record.

That ordinary event is a stronger sign of implementation success than a perfect migration-day screenshot.

24.81 What Should Happen If a New Contract Arrives Two Weeks Later?

Contracting triggers the security-change process. Redwood determines what information and requirements the new contract introduces. Program management explains the workflow and subcontractors.

The team compares the new work with the existing architecture. If it fits the established environment, the change may primarily involve authorization and documentation. If it introduces a new information type, application, location, provider, or sharing relationship, scope and architecture are reviewed.

Summit Ridge implements approved technical changes. Documentation and evidence are updated. The new work does not bypass security merely because the CMMC implementation project was declared complete.

This demonstrates why contract intake is part of continuous readiness.

24.82 How Should Costs Be Managed Without Sacrificing the Program?

Redwood should separate required security outcomes from particular products. This allows the organization to compare technical approaches and avoid buying overlapping capabilities simply because each vendor uses compliance language.

Cost analysis includes implementation and long-term operation. A cheaper product that requires extensive manual work may cost more over three years. An enclave that reduces license count may create support complexity. A premium managed service may reduce internal staffing needs but increase provider dependency.

Management should understand which costs reduce risk, which satisfy business or contractual needs, and which are convenience. Summit Ridge should be transparent about licenses, labor, third-party services, and optional enhancements.

Budget constraints do not eliminate requirements, but architecture and sequencing can often reduce waste.

24.83 How Does a Very Small Company Do This With Two IT People?

A small company needs simplicity and clear external support. It may rely heavily on an MSP, SOC, cloud provider, and specialist advisors. The internal team focuses on business authorization, contract understanding, provider governance, and the technical responsibilities it deliberately retains.

Standardization becomes especially important. A small company should avoid five ways to configure laptops and three unrelated file-sharing platforms. Repeatable builds and centralized management reduce the amount of knowledge two administrators must hold.

External providers should be selected for operational fit, not just product features. If the internal team cannot retrieve evidence or understand the service, outsourcing can create dependency without visibility.

The small-company model can be effective when responsibilities are explicit and the architecture is intentionally constrained.

24.84 How Does a Larger MSP Scale This Across Many Customers?

Summit Ridge creates a standard secure service baseline and then records customer-specific overlays. The baseline covers technician identity, RMM protection, credential management, ticketing, endpoint operations, vulnerability workflow, backup, monitoring integration, and evidence.

Each customer profile records its cloud environment, contractual context supplied by the customer, CUI workflow, approved technologies, escalation contacts, maintenance windows, exceptions, and responsibility assignments.

Automation operates against explicit customer groups and safeguards. Evidence remains segregated. Technician access is role-based and customer-specific where appropriate.

Scaling succeeds when standardization reduces error without erasing differences. Chapter 21's multi-customer principles and Chapter 22's technology-stack principles become operational inputs to this Day-One model.

24.85 What Should Be Tested Before a Formal Readiness Review?

The team tests identities, privileged access, endpoint enrollment, asset reconciliation, vulnerability detection and remediation, patch exceptions, backup restoration, log-source health, incident escalation, user termination, provider responsibilities, documentation accuracy, and evidence retrieval.

It also tests the business workflow. Can an engineer receive protected information through the approved path, work with it using approved systems, collaborate appropriately, and send it to an authorized recipient without leaving the designed environment?

Failures are corrected and retested. The team does not hide them. A readiness review should see a program that has already learned from internal testing.

The Random Tuesday approach from Chapter 23 can be used before formal assessment preparation: select representative evidence and ask whether the organization can explain it today.

24.86 How Do We Avoid the Last-Minute Evidence Scramble?

Every implementation task should identify its evidence before closure. A firewall change is not complete until implementation and verification are recorded. A new endpoint is not complete until security coverage is confirmed. A policy is not complete until the associated operating process exists.

Monthly evidence checks begin before the assessment. Redwood samples records from Summit Ridge, Beacon, and internal functions. Missing evidence is treated as a process problem rather than a document-collection problem.

By the time formal assessment preparation begins, the organization is curating evidence it already has. It may organize, label, and select samples, but it should not need to invent months of operational history.

This is the practical meaning of evidence by design.

24.87 What Is the Final Day-One Blueprint?

Day One begins with contracts and information. Discovery reveals flows, systems, people, providers, and unknowns. Scope defines the environment to be protected. Inventory establishes the population. The responsibility matrix assigns ownership. Gap assessment identifies what is missing. Target architecture defines the intended system.

Phase Two implements identity, endpoints, networks, cloud, applications, monitoring, vulnerability management, patching, backup, collaboration, and provider integrations. Every implementation is tested and produces evidence.

Phase Three challenges the environment through Operational Acceptance Testing, corrects failures, transfers knowledge, delivers documentation, and assigns permanent owners.

The program then enters continuous readiness. New contracts, people, systems, vulnerabilities, providers, and service changes are absorbed through the operating model rather than becoming uncontrolled drift.

This sequence is not a guarantee of a particular assessment outcome. It is a disciplined method for building an environment that can protect information, demonstrate its controls, and remain maintainable after the implementation project ends.

24.88 Closing: From an Empty Whiteboard to a Living Security Program

At the beginning of this chapter, Redwood had a business opportunity and a question. It did not yet have a trustworthy map of its CUI, a defined boundary, a responsibility model, a target architecture, an evidence plan, or an operating rhythm.

By the end, the organization can explain why the program exists, where protected information moves, which systems and providers participate, who performs each major function, how the technology was implemented, how the receiving team proved it could operate the environment, and how evidence will continue to be produced.

Summit Ridge has also changed. It is no longer simply an IT provider installing products. It understands its role in a customer's security architecture, protects its own administrative control planes, produces evidence for assigned services, respects customer-specific authority, and knows where its responsibility ends.

The deepest lesson is that CMMC implementation is not a sequence of purchases. It is the construction of an operating system for security responsibility. The contractor, MSP, security providers, cloud providers, and assessors occupy different roles, and success depends on connecting those roles without confusing them.

Build for the Tuesday after the project ends. If the environment can absorb that Tuesday's new employee, failed agent, new vulnerability, customer request, cloud change, and security alert while preserving control and evidence, the Day-One program has become a living security program.

Chapter 24 Comprehensive Implementation Pass: Answering the Questions Behind the Questions

The previous pass established what a contractor and MSP must do from Day One through operational handoff. This pass goes one level deeper. It focuses on the questions that appear when a reader attempts to perform the work rather than merely understand the roadmap. Each section therefore connects the decision to the actual people, records, tools, failure conditions, escalation paths, verification steps, and evidence that make the decision operational.

24.89 What Should Redwood Have in Its Hands at the End of the First Week?

By Friday of the first week, Redwood should not expect to have a completed SSP or a finished CMMC environment. It should expect to have control of the project. That means an accountable internal leader, a working team, the known contract and solicitation sources, a preliminary list of government programs, a discovery schedule, a list of major providers, a decision log, and an issue register containing the important unknowns.

The first week should also produce a preliminary map of where protected information may exist. The map can be imperfect. Its purpose is to guide interviews and technical discovery. If engineering says files arrive through a customer portal and are then placed on a file server, Summit Ridge can begin identifying the server, endpoints, backup path, and administrative systems connected to that workflow.

Redwood should also establish an immediate-risk lane. Discovery should not wait thirty days to correct an obvious high-risk condition. If the team finds shared administrator passwords, unsupported Internet-facing systems, or a known unprotected CUI repository, management assigns immediate remediation while the broader design continues.

The first-week evidence is modest but meaningful: kickoff record, ownership assignments, contract-source list, initial diagrams, discovery notes, decisions, and remediation tickets. The company has not completed CMMC; it has established governance over the journey.

24.90 What Should the Second Week Look Like?

The second week should deepen information-flow and asset discovery. Redwood interviews the people who actually perform protected work rather than relying only

on managers. Summit Ridge reconciles technical inventories. Contracting clarifies program requirements and identifies subcontractor relationships.

The team walks representative workflows at the keyboard. An engineer demonstrates how a drawing arrives, where it is downloaded, how it is edited, where the output is saved, and how it is transmitted. The team notes every system and provider touched. This practical demonstration often reveals more than a questionnaire.

Unknowns become decisions or assigned research. If a legacy application cannot operate in the proposed target cloud, the issue is raised before architecture is finalized. If an external provider's role is unclear, Redwood requests the necessary service and security information.

At the end of the second week, the organization should be able to draw a more credible current-state architecture and identify the most important gaps between current practice and the intended protected environment.

24.91 How Do We Interview Employees Without Making Them Afraid to Tell the Truth?

Discovery works only when employees believe the purpose is to understand the workflow, not to punish them for revealing inconvenient practices. Management should explain that the organization is trying to build a usable secure process and needs to know how work is actually performed.

Instead of asking, 'Do you ever use unapproved file sharing?' the interviewer asks, 'Show me what you do when a file is too large for email.' Instead of asking, 'Do you store CUI locally?' ask, 'After you download the drawing, where do you open and save it?' Demonstration produces better information than compliance-oriented yes-or-no questions.

If an employee reveals an unsafe workaround, the team asks why the workaround exists. Perhaps the approved service rejects large files, a subcontractor cannot access the portal, or remote performance is poor. Correcting the security problem may require correcting the usability problem.

The discovery record should focus on the process and remediation. The objective is to make the approved path become the natural path.

24.92 How Do We Determine Whether a System Really Needs CUI Access?

Access should follow business need. Redwood identifies which roles and projects require protected information and then maps those needs to systems. A receptionist may need corporate email but no CUI repository. An engineer may need project files but no tenant-wide administration. A project manager may need collaboration access but not engineering server administration.

The design should avoid granting broad access simply because it is easier to manage. Groups, roles, project memberships, and application permissions can express business authorization more precisely.

During implementation, Redwood selects representative users and tests access. The engineer should reach the assigned project but not an unrelated project. The standard user should not gain administrative access. An unauthorized device should behave according to the designed policy.

Periodic review later asks whether the business need still exists. This connects Day-One access design to Chapter 23's continuous-readiness access reviews.

24.93 What Exactly Does 'Least Privilege' Mean for an MSP Technician?

Least privilege does not mean technicians receive so little access that they cannot support the customer. It means access is limited to what the technician's role and current responsibilities require, and broad privilege is not granted merely for convenience.

Summit Ridge may create support tiers or customer-specific roles. A help-desk technician may reset passwords and assist endpoints without possessing tenant-wide global administration. A cloud engineer may receive elevated rights needed for a change. A security responder may need endpoint isolation capability without full billing or collaboration administration.

Where the platform supports just-in-time or time-limited elevation, the MSP can reduce permanent privilege. Where it does not, Summit Ridge compensates through role design, approvals, monitoring, strong authentication, and frequent review.

Evidence includes technician-role definitions, current assignments, access-review records, privileged activity logs, and offboarding records.

24.94 What If the MSP Uses a Shared Administrator Account Today?

The team should first understand why the shared account exists and where it is used. It may be embedded in a legacy process, vendor application, firewall, or emergency procedure. Simply deleting it can create an outage.

The target state should improve attribution and control. Individual administrative identities are preferred where the technology supports them. Shared emergency credentials, if necessary, receive strong protection, limited use, monitoring, and documented access procedures.

Summit Ridge migrates systems in a controlled sequence. It creates individual access, tests it, updates automation or dependencies, removes routine reliance on the shared account, and verifies that logs identify individual actions.

If a legacy platform cannot support individual administrators, the limitation becomes a documented risk and the surrounding controls are strengthened until the system can be replaced or redesigned.

24.95 How Do We Design the Privileged Credential Vault?

A credential vault should protect secrets while supporting accountable use. Summit Ridge decides which credentials belong in the vault, who can retrieve or use them, whether checkout requires approval, how access is logged, and how secrets are rotated.

The vault itself becomes a security-critical system. Strong authentication, least privilege, monitoring, recovery, administrative separation, and vendor/service evaluation matter because compromise can expose many customer environments.

Redwood should know which of its privileged credentials are held by Summit Ridge and what happens when the service relationship ends. Offboarding must return, rotate, or invalidate credentials as appropriate.

Operational Acceptance Testing can include retrieval of a test credential through the approved process and verification that the access event is recorded.

24.96 How Do We Decide Which Logs Are Important?

The team begins with scenarios. If an administrator changes Conditional Access, which record would show it? If an attacker signs in from an unusual source, which identity events are available? If malware executes on a workstation, what endpoint telemetry exists? If a firewall rule changes, where is the administrative event recorded?

These scenarios produce a source list. Identity, endpoint, network, cloud administration, critical applications, security platforms, and remote-management systems often deserve attention, but the exact list follows Redwood's architecture.

Beacon defines which sources it monitors and which detections it creates. Summit Ridge defines which operational platform alerts it handles. Redwood understands what is not monitored so absence of monitoring is not mistaken for coverage.

Testing generates representative events and confirms arrival, timestamps, identity attribution, and searchability. Source-health monitoring then checks whether the pipeline continues working.

24.97 How Do We Know Whether Our SIEM Is Actually Useful?

A SIEM is useful when it helps answer security questions and supports timely detection and investigation. Ingesting terabytes of data without defined detections, ownership, or response does not create an effective monitoring capability.

Beacon and Redwood identify priority scenarios: privileged-account misuse, suspicious authentication, endpoint detections, loss of security tooling, significant administrative changes, and network events relevant to the architecture. Detection content is mapped to those scenarios.

The team measures whether alerts reach a human, whether context is sufficient, whether false positives overwhelm analysts, and whether the escalation path reaches Summit Ridge or Redwood when action is required.

Periodic exercises validate the complete chain from event generation through detection, investigation, escalation, containment, and evidence.

24.98 How Do We Decide Patch Deadlines?

Patch deadlines should reflect the organization's vulnerability and change-management model rather than a single arbitrary number applied to every system. Severity, known exploitation, exposure, system criticality, information handled, and vendor guidance all influence urgency.

Redwood can establish target windows for ordinary updates and an emergency path for actively exploited or unusually consequential vulnerabilities. Summit Ridge needs authority and maintenance windows to execute those expectations.

Exceptions require an owner, reason, mitigation where appropriate, and review date. A deadline without an exception process encourages technicians to hide systems that cannot meet the deadline.

Metrics should show the remaining exceptions and their age, not merely the percentage patched.

24.99 What Happens When Patching Breaks an Engineering Application?

Summit Ridge first stabilizes the business service according to the change and recovery procedure. If rollback is necessary and authorized, the team restores the known working state. The security issue then remains open; rollback does not erase the vulnerability.

Redwood, Summit Ridge, and the application vendor determine whether a compatible patch, configuration mitigation, isolation, or application upgrade is available. Beacon may increase monitoring while the condition remains.

The decision record explains the tradeoff. Management understands the operational consequence and security exposure rather than receiving only a technical error message.

Once corrected, the team verifies both application functionality and security state. The lesson may lead to improved predeployment testing for future patches.

24.100 How Do We Know a Backup Is Protected From the Same Attack as Production?

Redwood examines whether production administrators can also delete backups, whether backup credentials are separate, whether immutability or protected copies are available where appropriate, whether the backup platform is monitored, and whether recovery access survives a primary identity compromise.

The architecture should avoid a single compromised identity having unrestricted power over both production and recovery wherever practical. The exact design depends on the backup platform and environment.

Summit Ridge tests recovery using the credentials and procedures expected during an incident. A backup that exists but cannot be accessed when the primary directory is unavailable may not meet the recovery design.

Evidence includes configuration, access review, backup success, restoration tests, and remediation of failed tests.

24.101 How Do We Decide Who Can Approve Security Exceptions During Implementation?

Redwood should define exception authority before exceptions begin accumulating. Technical staff can identify the issue and propose mitigations, but acceptance of material business risk belongs to the appropriate management authority.

The exception record identifies the requirement or baseline condition, affected assets, reason, risk, compensating measures, owner, approval, start date, and expiration or review date. Temporary migration exceptions should not silently become permanent.

Summit Ridge tracks technical exceptions it manages and escalates approaching expiration. Redwood reviews whether the business still needs the exception.

Closing the exception requires verification that the approved condition has actually been removed or replaced.

24.102 What If a Required Security Tool Conflicts With Production?

The team first confirms the conflict. An engineering application may fail when EDR blocks a behavior, but the correct response is not automatically to disable EDR for the entire engineering department.

Summit Ridge and the security vendor examine the detection, process, file, behavior, and scope. The application vendor may provide guidance. A narrowly scoped exclusion may be possible, but the team considers what protection is lost and whether monitoring can compensate.

Redwood approves material exceptions affecting business and risk. The exclusion receives an owner and review date. Future application upgrades should trigger reevaluation.

Testing verifies that the application works and that the security product continues protecting the rest of the intended environment.

24.103 How Do We Build Change Management Without Slowing the Company to a Halt?

Not every change requires an executive meeting. Redwood and Summit Ridge classify changes. Routine pre-approved maintenance follows standard procedures. Normal changes receive documented review and scheduling. High-risk or architecture-changing changes receive deeper security and business review. Emergency changes use predefined authority and retrospective review.

The purpose is to make consequential changes visible, not to create bureaucracy around every printer update. The change process should capture what is changing, why, affected systems, risk, testing, approval, implementation, rollback, and verification at a level appropriate to the change.

Security-impact questions help identify when CMMC documentation or scope may need review. Does the change introduce a new provider, new CUI flow, new privileged path, new external connection, or new system category?

This makes change management the mechanism that keeps the Day-One architecture aligned with the live environment.

24.104 How Do We Handle Emergency Changes During the Implementation Project?

Implementation itself can create emergencies. A migration may interrupt authentication, a firewall change may block a critical customer connection, or an endpoint policy may affect production.

The project establishes emergency authority and rollback before major changes. Summit Ridge knows which technical actions it can take immediately. Redwood provides business contacts. The implementation provider knows how to restore the prior configuration.

After stabilization, the team documents what happened and decides whether the emergency fix should remain. Temporary firewall rules, exclusions, or elevated roles are especially important to review.

The incident becomes a design lesson. A failed change can reveal missing testing, dependency discovery, or rollback planning.

24.105 What Should the Help Desk Know About CMMC Customers?

Help-desk staff do not need to become compliance assessors, but they need enough customer context to avoid unsafe shortcuts. Summit Ridge marks Redwood as a controlled customer profile with approved support methods, escalation contacts, and restrictions.

A technician should know whether remote support requires a specific tool, whether software installation needs approval, whether CUI may appear on screen during support, how to handle screenshots or attachments, and when a request involving access must be escalated.

Ticket templates can prompt the right information without forcing technicians to memorize every rule. Training explains why the prompts matter.

Quality review samples tickets to determine whether technicians are following the customer-specific operating model.

24.106 What If a Technician Accidentally Uses the Wrong Customer Tool or Tenant?

The immediate priority is to stop the action and determine what occurred. Did the technician merely open the wrong portal, or was data copied, a script executed, or a configuration changed? Summit Ridge preserves logs and investigates the scope.

Redwood is notified according to the incident and service model if its environment or information may have been affected. Corrective action restores any changed configuration and addresses data handling if information crossed boundaries.

The MSP then asks why the error was possible. Customer naming, browser profiles, administrative workstations, role separation, automation targeting, and technician workflow may need improvement.

A cross-customer mistake is not merely an individual training issue. It tests the MSP's multi-tenant safety design.

24.107 How Do We Validate Customer Separation in the MSP Stack?

Summit Ridge examines each multi-tenant platform: RMM, PSA, documentation, credential vault, backup, EDR, vulnerability management, and monitoring. It determines how customers are logically separated and which roles can cross those boundaries.

Testing uses non-production or controlled scenarios to confirm that a Redwood technician role cannot accidentally view another customer's secrets or execute actions outside the intended customer. Automation targeting receives special attention.

Evidence includes role configuration, access review, platform logs, and test results. Provider limitations are documented.

Customer separation is maintained continuously because new technicians, platform updates, and migrations can alter the access model.

24.108 How Do We Decide What Belongs in the Ticket Versus the SSP?

The SSP describes the system and how security requirements are implemented. A ticket records a particular operational event, change, incident, request, or remediation. They serve different purposes.

If Summit Ridge patches a server, the ticket records that specific work. The SSP does not need to list every patch. If Redwood changes the architecture so a new vulnerability platform becomes the permanent implementation, the SSP may need updating because the system description changed.

Procedures sit between them. The procedure describes how patching normally works. Tickets demonstrate that the procedure was performed. The SSP explains the broader implementation.

Understanding these layers prevents the SSP from becoming an unreadable event log and prevents tickets from being mistaken for complete system documentation.

24.109 How Do We Decide When a Diagram Must Be Updated?

A diagram should be updated when a change makes the existing representation materially misleading. Adding a major network segment, provider connection, security service, CUI repository, cloud environment, or trust boundary generally deserves review.

Minor endpoint replacement does not require redrawing the enterprise architecture if the logical design is unchanged. The organization defines an appropriate level of abstraction.

Change management can include a documentation-impact question. The implementer indicates whether diagrams, SSP sections, procedures, inventory, or responsibility records need revision.

Periodic validation compares diagrams with live configuration to catch changes that bypassed the process.

24.110 How Do We Handle Printers, Scanners, and Multifunction Devices?

These devices can be overlooked because they are not traditional workstations, yet they may receive, store temporarily, scan, print, or transmit protected information. Redwood identifies where such devices participate in CUI workflows.

The team examines network placement, administrative access, stored jobs, address books, scan-to-email or scan-to-folder configuration, firmware, logging where available, and disposal or replacement procedures.

If a device cannot meet the intended security model, Redwood may restrict its use, isolate it, replace it, or redesign the workflow.

The important lesson is that scope follows function. A device does not become irrelevant merely because it looks like office equipment.

24.111 How Do We Handle Mobile Devices?

Redwood first decides whether mobile devices are necessary for protected workflows. If they are not required, policy and technical controls can reduce unnecessary exposure. If they are required, the organization designs management, authentication, application, storage, encryption, remote-wipe, and access controls appropriate to the use.

Summit Ridge verifies enrollment and compliance before protected access is enabled. Lost-device procedures define reporting, session revocation, remote actions, and incident review.

Personal devices require especially deliberate decisions. Convenience should not silently create an unmanaged CUI path.

Operational evidence includes device population, management state, access policy, and incident records.

24.112 How Do We Handle Remote and Hybrid Workers?

Remote work extends the protected environment beyond the office. Redwood identifies what work can occur remotely, which devices are authorized, how users connect, whether printing is permitted, how physical privacy is handled, and which support methods are allowed.

Summit Ridge implements the technical access model using managed devices, authentication, secure connectivity, endpoint controls, and monitoring according to the architecture.

The team tests real home-office workflows rather than assuming office controls automatically transfer. A user may have a managed laptop but an unapproved local printer or file synchronization service.

Training explains practical expectations, and periodic review looks for exceptions created by convenience.

24.113 How Do We Handle Physical CUI?

CMMC technology discussions can obscure paper and other physical forms. Redwood maps where protected information may be printed, received, stored, transported, discussed, or destroyed.

Physical procedures address authorized areas, storage, visitor handling, printing, clean-up, transport, and destruction according to applicable requirements and organizational design.

Summit Ridge may have little or no responsibility for these controls, which demonstrates why an MSP cannot own the entire CMMC program.

Redwood's evidence comes from its physical security and business processes, while the SSP connects those processes to the overall system boundary where appropriate.

24.114 How Do We Handle a Subcontractor That Says 'We Are CMMC Ready'?

Redwood should determine what the contract requires of the subcontractor and obtain the information needed to support that decision. Marketing language is not a substitute for required status, flowdown, or security responsibility.

The business relationship defines what information the subcontractor will receive and through which system. Technical access is not granted until the contractual and security onboarding steps are complete.

Summit Ridge can implement the approved identity and exchange mechanism, but it should not decide whether the subcontractor satisfies contractual eligibility.

Offboarding is planned at the beginning so project completion removes access and closes the information-sharing path.

24.115 How Do We Handle an MSP Subcontractor?

Summit Ridge may rely on its own SOC, backup provider, cloud platform, or specialist subcontractor. Redwood needs visibility into provider relationships that materially affect the services supporting its environment.

The responsibility model should not stop at the MSP's logo. If Beacon performs monitoring, the documentation identifies that function. If another provider stores backups, the service and security implications are evaluated.

Summit Ridge remains responsible for the service commitments it makes to Redwood, while each underlying provider has its own role. Contractual and CMMC treatment should be evaluated using current applicable requirements.

This prevents hidden fourth-party dependencies from appearing only during an incident or assessment.

24.116 How Do We Decide Whether Internal IT or the MSP Performs a Task?

The decision considers capability, access, availability, accountability, cost, and evidence. Redwood may retain user authorization and application ownership while Summit Ridge performs endpoint administration. Another contractor may retain cloud administration internally.

The responsibility should match reality. Assigning Redwood a control because the policy template says 'IT Department' is meaningless if Summit Ridge actually performs the work.

Shared tasks should define the handoff. Redwood approves a new employee; Summit Ridge provisions access. Beacon recommends endpoint isolation; Summit Ridge executes it; Redwood receives notification according to severity.

The matrix should be understandable enough that a new employee can determine who to contact without knowing the project's history.

24.117 What Does a Good Daily Operating Rhythm Look Like After Implementation?

Daily work focuses on conditions that can become security gaps quickly: high-priority alerts, failed security agents, failed backups, critical vulnerability notifications, identity events, significant service failures, and incident queues.

Beacon handles its monitoring responsibilities. Summit Ridge handles managed-service exceptions. Redwood receives escalations requiring business decisions or incident participation.

The daily rhythm is exception-driven rather than a ritual review of every green dashboard. Automation can reduce noise, but unresolved exceptions remain visible until disposition.

Tickets and incident records capture investigation, action, verification, and escalation.

24.118 What Does a Good Weekly Rhythm Look Like?

Weekly review looks beyond today's emergencies. Summit Ridge reviews aging vulnerability and patch exceptions, devices missing expected coverage, backup failures, open changes, unresolved incidents, and onboarding or offboarding tasks.

Redwood reviews items awaiting business action. A server may remain vulnerable because management has not approved downtime. A subcontractor may be waiting for authorization. A policy exception may approach expiration.

The team asks whether recurring failures indicate a systemic problem. Five separate missing-agent tickets may mean the endpoint-build process is broken.

Weekly review converts accumulated operational noise into improvement.

24.119 What Does a Good Monthly Rhythm Look Like?

The monthly service and security review connects technical operations to management. Summit Ridge presents unresolved exceptions, coverage reconciliation, vulnerability trends, patching, backup and recovery results, significant changes, incidents, and upcoming technical risks.

Redwood brings business changes: new contracts, staffing, providers, locations, applications, subcontractors, and CUI workflows. The meeting therefore works in both directions.

Decisions receive owners and due dates. The meeting should not become a slideshow of green percentages. It should focus on what is outside the intended state and what the organization is changing.

The record becomes governance evidence and an input to quarterly review.

24.120 What Does a Good Quarterly Rhythm Look Like?

Quarterly review tests accumulated authority and architecture. Privileged access, provider relationships, major diagrams, security-platform coverage, recovery testing, documentation, and recurring exceptions receive deeper review.

Redwood may sample completed user lifecycles, changes, incidents, and evidence retrieval. Summit Ridge reviews technician access to Redwood. Beacon confirms monitoring sources and escalation performance.

The organization also looks ahead. Upcoming contracts, migrations, renewals, end-of-life technology, and major vendor changes are considered before they become emergencies.

Quarterly review is where operations and strategy meet.

24.121 What Does a Good Annual Rhythm Look Like?

The annual review asks whether the entire program still describes the business. Redwood revisits contracts, information flows, scope, providers, policies, SSP, responsibility matrix, architecture, training, incidents, exceptions, and evidence.

Summit Ridge supplies the year's operational history and identifies persistent weaknesses. Management evaluates whether staffing, architecture, or service levels need change.

Applicable annual affirmation and assessment obligations are handled according to current requirements and the contracts at issue. The program should have generated the underlying evidence throughout the year.

The annual review closes the loop back to Day One: what changed about the business, and does the security program still fit it?

24.122 How Do We Measure Whether the Program Is Improving?

Useful measures describe control health and unresolved risk. Examples include unexplained asset discrepancies, stale security agents, aged critical vulnerabilities, overdue access removals, failed backup jobs, restore-test outcomes, aging exceptions, and incident-response timing.

Metrics need context. Ninety-nine percent endpoint coverage sounds excellent until the missing one percent is the engineering server that stores the most sensitive project data.

Trends matter. If patch exceptions decrease while restore-test failures increase, management sees where attention should shift.

Metrics support decisions; they do not replace evidence or professional judgment.

24.123 How Do We Know the MSP Is Meeting Its Commitments?

Redwood compares the service agreement and responsibility matrix with observable operations. Are expected devices managed? Are vulnerabilities becoming tickets? Are backups monitored and tested? Are incidents escalated within the agreed model? Are technician privileges reviewed?

Monthly and quarterly reviews provide evidence. Redwood can also sample individual events: choose a failed backup and trace response; choose a terminated user and trace MSP actions; choose a vulnerability and trace remediation.

Persistent service gaps trigger corrective discussion rather than waiting for assessment. If the MSP cannot provide evidence for a responsibility it claims to perform, the operating model needs attention.

Provider governance is therefore an ongoing contractor responsibility.

24.124 What If Redwood Wants to Change MSPs?

Provider transition is a security project because the outgoing MSP may hold credentials, RMM agents, documentation, backup access, tenant roles, API tokens, and institutional knowledge.

Redwood creates a transition inventory before termination. The incoming provider receives authorized documentation and access through controlled handoff. The outgoing provider's identities, tools, integrations, and secrets are removed or rotated.

Device populations are reconciled so no endpoint loses management or protection during the change. Historical evidence and ticket records needed by Redwood are preserved according to agreements and requirements.

The transition is complete only when the old provider can no longer access the environment and the new operating model has been validated.

24.125 What If the Implementation Provider and Long-Term MSP Disagree?

Disagreement should be resolved against the approved architecture, requirements, current documentation, vendor facts, and Redwood's business decisions rather than organizational ego.

The implementation provider may understand the migration design better; Summit Ridge may understand long-term operational constraints better. Both perspectives matter. Redwood owns the decision where business and risk are involved.

A technical design that cannot be maintained reliably deserves reconsideration. Conversely, an MSP preference for familiar tooling should not override a requirement the familiar tool cannot satisfy.

Decisions and rationale are documented so the same debate does not recur after personnel change.

24.126 What If Redwood Cannot Afford Everything at Once?

Redwood should identify which requirements and risks must be addressed for the intended work and which improvements can be sequenced. Management should not treat an unmet mandatory condition as optional merely because funding is difficult.

The roadmap can stage migrations, consolidate tools, reduce scope, simplify architecture, or change business workflow to make the program sustainable. A smaller well-controlled environment may be more affordable than attempting to secure every legacy system.

Where current rules permit limited POA&M treatment for particular requirements and circumstances, Redwood follows those exact rules rather than assuming every gap can be deferred. Level 1, for example, does not permit POA&Ms under the CMMC program.

The budget conversation should therefore influence architecture early, not become an excuse at the end.

24.127 How Do We Avoid Building a Program That Only One Person Understands?

Key knowledge is converted into documentation, runbooks, diagrams, responsibility records, and cross-training. Administrative credentials and recovery information are stored through controlled organizational processes rather than personal memory.

At least one alternate should understand critical functions. A two-person IT team may rely on Summit Ridge for backup expertise; Summit Ridge may cross-train technicians for Redwood. The design identifies single-person dependencies.

Operational Acceptance Testing is especially useful because it exposes knowledge concentration. If only the implementation engineer can perform a restore or explain Conditional Access, the system is not ready for handoff.

Personnel resilience is part of maintainability.

24.128 What If the Assessor Asks a Question We Did Not Rehearse?

The correct response is not to guess. The person should explain what they know, identify the responsible owner if the question belongs elsewhere, and retrieve authoritative evidence where appropriate.

Redwood should train participants to understand their actual roles rather than memorize scripts. An engineer explains how protected files are handled. Summit

Ridge explains the technical service it performs. Management explains authorization and governance.

Unexpected questions are less threatening when documentation matches reality. The organization does not need to remember a fabricated story.

Assessment preparation should therefore build understanding, not theater.

24.129 What If the Evidence and the Interview Answer Disagree?

The discrepancy should be investigated. The document may be stale, the employee may misunderstand the process, the system may have changed, or the implementation may not match policy.

Before formal assessment, internal validation deliberately searches for these contradictions. The team compares interviews, technical configuration, tickets, policies, and SSP descriptions.

Correction depends on which source reflects the approved intended state. Sometimes the technology is wrong; sometimes the procedure is obsolete; sometimes both need change.

The final evidence package should tell one coherent, truthful story.

24.130 What If a Control Works Technically but Nobody Owns It?

A technical control without ownership will eventually decay. A firewall rule can remain correct today, but who reviews it after the application is retired? EDR can be deployed, but who investigates missing agents? A SIEM can collect logs, but who responds to alerts?

The responsibility matrix assigns permanent ownership before handoff. The owner may be Redwood, Summit Ridge, Beacon, or another provider, but the performer and escalation path must be known.

Monitoring and recurring tasks are then scheduled or automated. Evidence ownership is also assigned.

This converts implementation success into operational durability.

24.131 What If Someone Owns a Control but Has No Evidence?

The team asks whether the process is actually occurring and whether the system can produce an authoritative record. Sometimes the control works but evidence retention

or retrieval was never designed. Other times the lack of evidence reveals that the activity is informal and inconsistent.

Summit Ridge may need to configure ticket automation, reporting, or retention. Redwood may need to document approvals. Beacon may need to preserve incident disposition.

Evidence should be produced as a byproduct of the process rather than manually recreated later.

After correction, the team performs the activity and verifies that the expected evidence is generated.

24.132 What If We Have Evidence but the Control Is Not Effective?

A pile of tickets can prove that technicians closed tickets; it does not prove that vulnerabilities were actually remediated. A screenshot can prove a policy existed at one moment; it does not prove devices received it.

Verification connects evidence to outcome. Vulnerability remediation is rescanned. Endpoint enrollment is reconciled. Access removal is tested. Backup restoration is performed. Log-source health is checked.

The evidence package should therefore include enough information to demonstrate both implementation and operation.

This distinction prevents compliance documentation from drifting away from security effectiveness.

24.133 How Do We Decide Whether to Automate a Process?

Automation is valuable when the process is repeatable, inputs are reliable, and failure can be detected. Summit Ridge may automate device enrollment checks, patch deployment, ticket creation, or account workflows.

High-impact automation needs safeguards. A script that changes every customer firewall or disables hundreds of accounts deserves stronger testing, targeting controls, approvals, and rollback than a script that collects inventory.

Automation should produce logs and exceptions. Silent automation failure is dangerous because staff may assume the task occurred.

The decision is not automation versus people. It is how people design, authorize, monitor, and verify automated work.

24.134 How Do We Test Automation Safely?

Summit Ridge begins with a controlled test population. Inputs, expected results, permissions, error handling, and rollback are defined. The team observes both success and failure.

Customer targeting is verified before broad execution. The script should not rely on ambiguous names or assumptions that could cross customer boundaries.

After deployment, monitoring confirms expected coverage and identifies failures. A successful script execution message is not enough if the endpoint configuration did not actually change.

Version control and change records preserve what automation was executed and why.

24.135 How Do We Handle Tool Replacement After Certification or Assessment?

Tool replacement is allowed; security programs are not frozen forever. The organization must manage the change so required functions, scope understanding, evidence, and operations remain intact.

Before replacement, Redwood and Summit Ridge identify what the old tool does, which integrations depend on it, what history must be retained, and how the new tool will be validated.

During transition, populations are reconciled. After transition, old agents, accounts, tokens, and integrations are removed. Documentation and evidence maps are updated.

The replacement demonstrates continuous readiness: change occurs without losing control.

24.136 What Does 'Ready' Actually Mean at the End of Chapter 24?

Ready does not mean nothing can fail. It means Redwood understands its current environment, has implemented the required operating model for the work at issue, knows its remaining conditions and exceptions, can demonstrate responsibilities, and can detect and respond when controls degrade.

Summit Ridge can perform its assigned services, retrieve evidence, support assessment activities, and maintain the environment without depending on undocumented project knowledge.

Employees can perform protected work through approved workflows. Management can make informed decisions. Providers know their boundaries. Documentation describes reality.

The organization has moved from a project that builds security to an operating program that maintains security.

24.137 The Final Comprehensive Walkthrough: A New Employee Joins Redwood

A new engineer, Elena, joins Redwood after implementation. Her manager identifies the projects she will support and authorizes the required access. HR triggers onboarding. Summit Ridge provisions her identity and licenses, applies the appropriate groups, and confirms MFA.

Elena receives a managed laptop. The device is inventoried, enrolled, encrypted, protected by EDR, added to RMM, included in vulnerability and patch management, and validated. Conditional Access recognizes the compliant device.

Elena completes required training and learns the approved CUI workflow. She can reach her assigned engineering repository but not another program. The onboarding ticket contains authorization and technical verification.

Thirty days later, the monthly access review samples Elena. Her access still matches the approved role. The ordinary employee lifecycle has generated security and evidence without an assessment project.

24.138 The Final Comprehensive Walkthrough: A Critical Vulnerability Appears

A critical vulnerability affects software on Elena's engineering workstation and several servers. Vulnerability management identifies the affected population. Summit Ridge verifies exposure and creates remediation work. Beacon reviews for related threat activity.

The workstation patch can be deployed immediately. One server requires downtime. Redwood approves an evening maintenance window. Another server cannot yet accept the patch because of application compatibility, so the team applies an approved mitigation and creates a time-bound exception.

After patching, Summit Ridge rescans or otherwise verifies remediation. The exception remains visible until the vendor-supported solution is available.

The complete lifecycle demonstrates inventory, detection, prioritization, business authorization, remediation, exception handling, verification, monitoring, and evidence.

24.139 The Final Comprehensive Walkthrough: Elena Leaves

Months later, Elena leaves Redwood. HR triggers the termination process. Her identity is disabled at the authorized time, sessions and access are revoked, project memberships are removed, and the laptop is recovered.

Summit Ridge checks application dependencies and finds that Elena also had access to a customer-specific engineering portal. That account is removed. The device is retired from active management only after data handling and disposition are complete.

A subsequent sample verifies that Elena no longer appears in active access populations. The organization does not depend on someone remembering every system because offboarding was designed and tested during Chapter 24 implementation.

The same program that securely brought Elena into the environment has securely removed her.

24.140 Final Closing: The Questions Have Become an Operating System

At Day One, every question felt separate: What is CUI? Which systems are in scope? Do we need GCC High? Who patches the servers? Who watches the logs? Who owns the SSP? What does the MSP do? What evidence do we need?

By the end of the implementation journey, those questions connect. Information determines scope. Scope informs architecture. Architecture assigns technology and providers. Responsibility defines operations. Operations create evidence. Evidence supports verification. Verification exposes failures. Corrective action improves operations. Change management keeps the documentation aligned.

That connected system is the real product of Chapter 24. The contractor has not purchased compliance. It has built a governable security environment. The MSP has not become the contractor. It has become an accountable operator of defined portions of that environment.

The next assessment, contract change, new employee, vulnerability, cloud update, or provider transition will test the system. If the organization can absorb those events

while maintaining security, responsibility, evidence, and awareness, the Day-One implementation has achieved its purpose.

Chapter 25

MSP CMMC Case Study: From Readiness to Certification

CMMC for MSPs: From Readiness to Certification
Authored by Dr. Charles Edwards

25.1 The Purpose of the Final Case Study

This chapter is intentionally different from the chapters that came before it. Instead of teaching one CMMC subject at a time, it places the reader inside a complete fictional engagement and asks every major concept in the book to operate together. The names, companies, people, contracts, and events in the case study are fictional. The technical and operational problems, however, are representative of situations a defense contractor and its MSP can encounter.

The contractor is Meridian Aerostructure Components, a seventy-five-person engineering and precision-manufacturing company. Meridian produces machined assemblies, engineering modifications, inspection packages, and technical deliverables for commercial customers and defense-industry primes. It has grown quickly. Its technology works well enough to support the business, but the environment was not originally designed around a formal CMMC operating model.

Meridian's MSP is NorthBridge Managed Technology. NorthBridge supports Microsoft 365, endpoints, servers, networking, remote administration, backup, vulnerability management, and the help desk. A separate fictional security provider, HarborWatch Security Operations, provides managed detection and security monitoring. A specialized government-cloud implementation firm, Federal Cloud Works, can be engaged if Meridian's target architecture requires that expertise. The names are deliberately generic and fictional; the lesson is the separation of roles.

The case begins before anyone knows exactly what must change. It ends months after the formal readiness milestone, on an ordinary Tuesday when a control fails. The reader will therefore see not only how an organization prepares, but whether the system it built can survive normal business.

25.2 The Trigger: A Contract Opportunity Changes the Conversation

Meridian's president receives a call from a prime contractor. The prime is preparing a new program and wants Meridian to bid on a manufacturing package. The work will include technical drawings and engineering information. During the pre-bid discussion, the prime asks Meridian for information about its cybersecurity posture and the CMMC requirements associated with the opportunity.

The president forwards the request to the operations director with a short question: 'Are we CMMC compliant?' The operations director forwards it to NorthBridge. NorthBridge's service manager answers carefully. Meridian has MFA, endpoint protection, managed firewalls, backups, patching, and several other security controls, but those technologies alone do not establish Meridian's complete CMMC status.

This is the first important decision in the case study. NorthBridge does not answer yes merely because its security stack is strong. It also does not answer no simply because Meridian has never called its environment a CMMC enclave. The MSP explains that Meridian needs to examine the contract requirements, information involved, scope, current practices, provider relationships, documentation, and evidence.

The president's original question therefore changes. The useful question is no longer 'Do we have enough security tools?' It becomes 'What does this work require, what information will we handle, what environment will handle it, and can we demonstrate that the required protections actually operate?'

25.3 Establishing the Team Before Establishing the Answer

Meridian names its operations director as the internal CMMC program owner. The president remains executive sponsor. Contract administration owns the solicitation and flowdown review. Engineering explains technical workflows. HR owns personnel triggers. NorthBridge owns the managed technical functions assigned by its agreement. HarborWatch owns the monitoring functions in its service. A readiness specialist is engaged to help Meridian interpret the program requirements and organize the readiness effort.

The team deliberately avoids giving the readiness specialist operational ownership of the environment. Advice, implementation, managed operation, business accountability, and formal assessment are different functions. The case study will keep those functions separate even when the same people participate in meetings.

The first project artifact is not an SSP. It is a responsibility-and-discovery record. It identifies who can answer contract questions, who understands engineering workflows, who can export device inventories, who administers the Microsoft tenant, who manages the firewall, who operates backup, who investigates security alerts, and who can approve business risk.

This small step prevents a recurring problem: a consultant asks the MSP a business question, the MSP guesses; the MSP asks the contractor a technical question, the contractor guesses; and the final documentation contains confident statements that nobody actually verified.

25.4 The Contract Review Changes the Technical Project

Contract administration and the readiness specialist review the solicitation information and the expected flowdown. They identify that the opportunity will

involve CUI and determine the cybersecurity and assessment expectations applicable to the opportunity. Because requirements can change over time and differ by solicitation, the team treats the actual solicitation and current authoritative rules as the source rather than relying on an old presentation.

This distinction is especially important in the September 2026 regulatory environment. DoD's current CMMC information states that Phase II requirements were suspended on July 13, 2026 and that Phase I self-assessment requirements remain in place. The current DoD page describes Level 1 annual self-assessment and Level 2 self-assessment every three years with annual affirmation under the Phase I posture. The team therefore avoids inventing a future third-party requirement that the current opportunity does not contain.

At the same time, Meridian understands that a future solicitation can specify a different required CMMC level or assessment type under the applicable acquisition rules. The company wants an architecture that can support its intended defense business rather than one designed only to survive today's questionnaire.

NorthBridge receives the outcome as a technical design input. It does not interpret the contract independently. This is the first visible example of contractor responsibility feeding MSP implementation.

25.5 The First CUI Workshop

The team selects one representative engineering package and asks the engineering manager to demonstrate what employees do today. The manager signs into the prime's portal, downloads a drawing, opens it on a company laptop, saves a working copy to an engineering file share, and explains how the team collaborates.

During the demonstration, an engineer mentions that large files are sometimes sent through a commercial file-sharing service because outside recipients have difficulty with email attachments. Nobody in the kickoff meeting knew this service was being used. The engineer is not trying to evade security; the approved workflow simply did not solve the business problem.

The discovery changes the project. The team now knows that protected information may leave the expected environment through an unreviewed service. Instead of blaming the engineer, Meridian asks why the workaround exists, which projects used it, what information may have been transferred, who has accounts, and what approved replacement can support the same workflow.

NorthBridge blocks no service impulsively during the meeting. Meridian first determines the business and information implications, preserves relevant facts, and

establishes an approved alternative. The eventual technical restriction is paired with a usable secure-transfer process. The case demonstrates an important principle: secure architecture has to support real work.

25.6 Following the Information Beyond the File Server

The workshop continues. Engineering files are backed up by NorthBridge. Selected folders synchronize to collaboration services. Engineers use a CAD application. A quality system stores inspection records. Some employees print drawings on a multifunction device near the manufacturing floor. A subcontract machine shop receives selected technical packages.

Every one of these facts creates another question. Does the backup service store CUI? Does the collaboration environment support the intended requirements? Does the CAD application create temporary local files? Does the multifunction device retain jobs? How is the subcontractor authorized? Which system records the transfer? Who administers each component?

The information-flow diagram expands from a simple portal-to-file-server arrow into a business process. The team marks sources, repositories, endpoints, applications, external recipients, backup, administrative paths, and monitoring.

This is the moment Meridian understands why a device inventory by itself could never define the CMMC environment. Scope emerges from information and security function, not merely from ownership stickers.

25.7 The Inventory Reconciliation Problem

NorthBridge exports its device population. RMM reports 119 managed endpoints and servers. EDR reports 116. Vulnerability management reports 114. The Microsoft device-management population contains 111 active records. Meridian's accounting asset list contains 126 computers.

The numbers are uncomfortable, but they are valuable. The team does not average them or choose the RMM number as authoritative. It reconciles them asset by asset.

Two accounting records belong to retired laptops still awaiting disposal. Three RMM records are stale. Two engineering workstations are missing the vulnerability agent. One recently rebuilt laptop has RMM but no EDR. A legacy manufacturing workstation is intentionally isolated from normal Internet access but still performs a business function and requires explicit treatment.

Each discrepancy becomes a disposition. The rebuilt laptop receives EDR and is verified. The vulnerability agents are repaired. Retired devices move through

disposition. The legacy workstation receives architectural review rather than being silently excluded.

The evidence is not simply the final inventory. The reconciliation tickets demonstrate that Meridian and NorthBridge can recognize when expected protection is missing.

25.8 The MSP Discovers Its Own Scope-Relevant Dependencies

NorthBridge initially describes itself as 'the MSP.' That label is too broad to be useful. The team decomposes the service. NorthBridge's RMM can execute commands on Meridian endpoints. Its credential vault stores privileged customer secrets. Its PSA contains support tickets. Its backup platform protects servers. Its technicians administer the Microsoft tenant. Its vulnerability platform scans managed assets.

HarborWatch receives endpoint and identity telemetry and performs monitoring. The backup platform is operated through another cloud provider. NorthBridge also uses a documentation platform containing network diagrams and administrative information.

The team now evaluates each provider and system by function. Some services process or store customer information; others provide security protection or privileged administration. The responsibility model records the actual relationship rather than pretending all responsibility stops at NorthBridge.

NorthBridge also reviews which technicians can access Meridian. It discovers that its senior-engineer group has broad access to every managed customer even though only four engineers routinely support Meridian. That design becomes an MSP remediation item.

25.9 The Responsibility Workshop

The project team opens a blank responsibility matrix and begins with user access. Meridian managers authorize access. HR supplies employment triggers. NorthBridge provisions technical access. Meridian's program managers approve project-specific CUI access. NorthBridge supplies identity and access evidence. Meridian periodically reviews whether business authorization remains appropriate.

Next comes vulnerability management. NorthBridge operates scanning and triage. Meridian approves downtime for production-sensitive remediation. Application vendors may be consulted. NorthBridge verifies remediation. Meridian receives unresolved-risk escalation.

For security monitoring, HarborWatch monitors agreed sources and investigates alerts. NorthBridge performs endpoint or infrastructure containment when authorized

by procedure. Meridian owns business and contractual decisions. Serious incidents trigger the broader incident-response process.

By the end of the workshop, 'shared responsibility' no longer means everybody is responsible. It means the handoffs are explicit.

25.10 The Gap Assessment Begins With Demonstration

The readiness specialist asks NorthBridge to demonstrate privileged administration. The MSP shows its vault, MFA, RMM, and tenant access. During the demonstration, the team finds an old emergency Microsoft administrator account excluded from a Conditional Access policy. The account was created during a migration and never removed.

The finding illustrates why documentation alone is insufficient. Meridian's access policy says MFA is required for administrative access. The live environment contains an exception that the current administrators did not know existed.

NorthBridge investigates before deleting the account. It confirms no application depends on it, reviews recent activity, establishes the approved emergency-access design, removes the obsolete exclusion, tests administrative access, and documents the correction.

The evidence package contains the finding, investigation, approved change, resulting configuration, and verification. The gap assessment has already improved security before a formal score is discussed.

25.11 A Second Gap: Backup Success Without Recovery Proof

NorthBridge's backup dashboard is almost entirely green. The service manager initially considers backup one of Meridian's strongest controls. The readiness specialist asks a different question: when did Meridian last restore an engineering application?

The answer is unclear. Individual files have been restored, but nobody can identify a recent test of the engineering file service as a business service. The team schedules a controlled recovery exercise.

The restore begins successfully, but the recovered application cannot authenticate because a dependency was not included in the original runbook. The backup data is intact; the recovery process is incomplete.

NorthBridge documents the dependency, updates the recovery sequence, repeats the exercise, and verifies that an authorized test user can access the restored data.

Meridian now has stronger evidence than a green backup dashboard: it has proof that the recovery procedure was challenged, failed, corrected, and successfully retested.

25.12 Designing the Target Environment

The gap assessment shows that Meridian has many useful security controls but lacks a coherent target architecture. The team considers whether to protect the broader enterprise or create a more constrained CUI environment.

Engineering workflow is the deciding factor. A narrow enclave would reduce some scope but require engineers to move repeatedly between environments and would complicate several applications. A broader controlled engineering environment costs more to manage but better matches the way Meridian performs the defense work.

The team documents the tradeoff instead of treating scope reduction as automatically superior. It identifies identity, endpoint, network, collaboration, engineering applications, secure transfer, backup, monitoring, vulnerability management, RMM, and administrative paths.

The architecture is then tested against representative work. Can an engineer receive a drawing, modify it, collaborate, produce an inspection package, send an approved deliverable, and recover the work after failure without leaving the designed environment? If the answer is no, the architecture is not finished.

25.13 The Microsoft Government Cloud Decision

Meridian's leadership has heard from several vendors that 'CMMC means GCC High.' The project team refuses to use that slogan as an architecture decision. It reviews the actual information, contractual obligations, additional regulatory considerations, Microsoft service commitments, eligibility, application compatibility, integrations, and long-term operations.

The team understands that GCC and GCC High are Microsoft government cloud environments, not CMMC certificates. Purchasing a government-cloud license does not implement endpoint security, business authorization, incident response, evidence, backup, or the rest of Meridian's program.

For the case study, assume Meridian's contract and data requirements lead the company to select a Microsoft Government environment appropriate to those requirements. The implementation is treated as a tenant and business-workflow migration. Federal Cloud Works assists with specialized tenant and migration tasks. NorthBridge participates from the beginning because it will operate the environment after handoff.

This last point prevents a common failure. The company that builds the environment and the company that maintains it cannot meet for the first time on the final day.

25.14 Identity Architecture Before Migration

Meridian defines administrative roles before moving production data. Ordinary user identities are separated from privileged administration according to the design. NorthBridge identifies the four technicians who require routine Meridian support and removes unnecessary broad customer access.

MFA and Conditional Access policies are designed around user and administrator scenarios. Emergency access is documented deliberately rather than created as an unexplained exclusion. Service identities and application dependencies are inventoried.

The team tests policy behavior using controlled accounts. An authorized user on a managed device reaches the intended resource. An unauthorized account does not. A privileged identity performs the administrative task and leaves an attributable log record.

Identity becomes the foundation for the rest of the migration rather than a cleanup task performed afterward.

25.15 The Application Compatibility Surprise

During pre-migration testing, Meridian discovers that a CAD-related integration depends on an authentication flow and endpoint assumption that will not work unchanged in the target environment. If the team had discovered this on migration weekend, engineering production could have stopped.

Federal Cloud Works, NorthBridge, Meridian engineering, and the application vendor analyze the dependency. They identify a supported configuration and test it with representative files. Where a temporary migration exception is needed, it receives an owner and expiration condition.

The project schedule changes by one week. Management initially dislikes the delay, but the program owner explains that the delay is evidence the design process is working. A hidden production dependency has been found while the organization still controls the timing.

The compatibility test and decision become part of the migration record and handoff documentation.

25.16 Endpoint Standardization

NorthBridge develops the Meridian controlled-endpoint build. A new device is entered into inventory, enrolled in management, encrypted, protected by EDR, connected to RMM, included in vulnerability and patch management, configured with approved applications, and tested against access policy.

Existing devices are reconciled against this baseline. The team does not assume that an installed agent means the service is healthy. Each expected platform must show the device as active and current.

An engineering workstation fails the enrollment sequence because an old management object conflicts with the rebuilt device. The technician removes the stale relationship, reenrolls the system, and verifies policy, EDR, vulnerability coverage, and access.

The failed enrollment is retained as an implementation lesson. NorthBridge updates the build procedure so technicians know how to recognize the condition on future devices.

25.17 Network and Remote Access

Meridian's network contains corporate user segments, engineering resources, manufacturing systems, wireless networks, printers, servers, and administrative infrastructure. The team documents permitted paths and reduces unnecessary connectivity.

Remote access is redesigned around managed identities and devices. Legacy paths are identified. One old vendor-support VPN account is found on a firewall. The vendor no longer supports Meridian, but the account was never removed.

NorthBridge disables the obsolete path after verifying it is unused and reviews other vendor access. The team establishes a process requiring sponsor, purpose, expiration, and review for future third-party remote access.

The firewall configuration, change ticket, and access procedure now tell the same story.

25.18 Logging and the Missing Firewall

HarborWatch receives identity and endpoint telemetry and selected network logs. During source reconciliation, an analyst notices that one Meridian firewall has not sent logs for four days.

No security alert says the firewall was attacked. The important event is the absence of expected telemetry. HarborWatch opens an escalation to NorthBridge.

NorthBridge finds that a certificate used by the log-forwarding connection expired after a configuration change. The firewall itself is functioning, but monitoring coverage is degraded. The technician renews the connection, verifies events at HarborWatch, and confirms the missing-source alert clears.

The incident becomes a central teaching example. A quiet SIEM can mean nothing bad happened, or it can mean the organization stopped seeing. Source health is therefore a control that needs monitoring.

25.19 Vulnerability Management Becomes a Workflow

The first comprehensive scan produces more findings than Meridian expected. Management sees the number and asks whether the project is failing. NorthBridge explains that discovery is the point of the scan.

The team triages findings by severity and context. Internet-exposed or high-consequence conditions receive urgent attention. Routine patches enter maintenance windows. Engineering systems that require compatibility testing receive coordinated remediation.

One critical finding affects a production server that cannot be restarted during a customer run. Meridian's operations director approves a short delayed maintenance window and interim mitigation. The exception is documented rather than hidden.

After maintenance, NorthBridge verifies the fix. The finding disappears from the affected population, and the ticket records authorization, implementation, and verification.

25.20 The Secure File-Transfer Problem Is Solved as a Business Problem

The commercial file-sharing workaround discovered in the first workshop cannot simply remain blocked without replacement. Meridian evaluates approved exchange methods compatible with its requirements and recipients.

The selected workflow is tested with a real-sized engineering package and a controlled external recipient. The team verifies authorization, transfer, access expiration, and audit information.

Engineering employees receive scenario-based training. They are told what to do when a recipient says the approved method is inconvenient. The answer is to escalate the business problem, not silently choose another service.

NorthBridge implements technical restrictions where appropriate, but Meridian owns the information-sharing authorization. The solution combines usability, governance, and technology.

25.21 The Subcontractor Question

Meridian's machining subcontractor needs selected technical information. The project team reviews the contractual flowdown and current requirements applicable to the information being shared. Meridian does not accept a statement that the subcontractor is 'cyber compliant' as sufficient by itself.

Contract administration determines what must be flowed down and what status or evidence is required for the subcontract relationship. NorthBridge implements the approved technical access only after Meridian authorizes it.

The subcontractor receives access to the specific exchange mechanism needed for the work rather than broad access to Meridian's environment. Project completion triggers access removal.

This case demonstrates that technical provisioning is the last step in a chain that begins with contractual and business authorization.

25.22 Writing Policies After Understanding the Work

Meridian now writes and revises policies around the operating model it has actually designed. Access policy describes authorization and privileged control. Configuration and change policy establishes authority. Incident response identifies roles. Media and information-handling procedures reflect engineering reality.

The team rejects copied language that would require nonexistent committees or tools. A small contractor does not become mature by pretending to have a large-enterprise bureaucracy.

Each policy statement is tested against operation. If Meridian says privileged access is reviewed periodically, who performs the review? Where is the population obtained? What happens when excessive access is found? Where is the record retained?

Policy becomes an executable management commitment rather than a ceremonial document.

25.23 Building the SSP From the Live Architecture

The SSP has been developing throughout the project, but it now receives a full reconciliation. The writers compare each major description with the live environment, diagrams, responsibility matrix, provider services, and technical demonstrations.

NorthBridge supplies accurate descriptions of the functions it performs. HarborWatch supplies the monitoring-service description. Meridian describes business authorization and internal processes. Federal Cloud Works does not remain listed as the permanent operator merely because it performed the migration.

One SSP section still says that all vulnerability remediation is performed within a fixed period. The live process contains risk-based prioritization and documented exceptions. The team corrects the language so the SSP describes the approved operating model accurately.

This is not weakening documentation. It is removing a false statement and replacing it with the real process that can be demonstrated.

25.24 Evidence by Design

The team builds an evidence map. Access claims point to authorization records, identity configuration, and reviews. Endpoint claims point to management platforms and reconciliation. Vulnerability claims point to scans, tickets, exceptions, and verification. Backup claims point to jobs and restore tests. Monitoring claims point to source health, investigations, and escalations.

Evidence owners are assigned. NorthBridge cannot assume Meridian will retain MSP platform history forever. Meridian cannot assume HarborWatch can instantly retrieve every old event without understanding the service.

The team samples evidence monthly. A random terminated user is traced. A random vulnerability is traced. A random firewall change is traced. A random endpoint is compared across security platforms.

By assessment preparation, evidence retrieval is normal work rather than an emergency.

25.25 The Employee Departure Test Arrives Early

During readiness work, a Meridian engineer resigns. HR sends the approved termination trigger. NorthBridge disables the central identity, revokes sessions, removes project access, and begins device recovery.

The offboarding review reveals that the engineer also had an account in a specialized engineering portal not federated with Meridian's main identity system. The account would have survived if the team had relied only on central directory disablement.

The portal is added to the offboarding dependency list. The account is removed, and the team searches for other direct application identities.

A real employee departure has become a validation exercise. The organization improves the process before assessment and retains evidence of the correction.

25.26 The Incident Tabletop

Meridian runs a tabletop scenario involving a compromised engineering workstation. HarborWatch detects suspicious activity and escalates. NorthBridge receives the alert and prepares to isolate the device. Meridian's incident lead determines business and contractual escalation.

The exercise exposes a practical problem: HarborWatch's after-hours contact list contains an old NorthBridge service manager. The technical detection works, but the human escalation chain is stale.

The contact list is corrected across the providers. The team then reruns the communication portion. HarborWatch reaches the right person, NorthBridge demonstrates the isolation workflow, and Meridian records the management decision path.

The lesson is that incident response is a system of people, authority, communications, technology, and evidence. A well-written plan with an obsolete phone number can still fail.

25.27 Operational Acceptance Testing Begins

Federal Cloud Works has completed the major cloud implementation. NorthBridge is expected to maintain the environment. Meridian refuses to accept the project based only on successful migration statistics.

The Operational Acceptance Test begins with a test employee. NorthBridge provisions the identity, assigns the approved license and groups, enrolls MFA, and confirms access. The technician then provisions a test laptop through the controlled build and demonstrates device management, encryption, EDR, RMM, vulnerability coverage, and Conditional Access.

Next, the team disables the user and verifies removal. It retrieves relevant logs and evidence. It restores a test file and application component from backup. It follows a simulated HarborWatch escalation.

The purpose is not to embarrass the receiving team. It is to prove that the people who will operate the environment can do so without the implementation provider standing beside them.

25.28 The OAT Failure

During the OAT, NorthBridge is asked to retrieve the configuration history for a Conditional Access change. The administrator can show the current policy but cannot immediately locate the historical evidence expected by the test.

The team marks the test as failed. Federal Cloud Works and NorthBridge identify where the audit information is available, confirm licensing and retention assumptions, document the retrieval procedure, and repeat the exercise with another controlled change.

The second test succeeds. NorthBridge updates its runbook and evidence map.

Meridian does not treat the initial failure as a reason to hide the OAT record. The failure demonstrates why operational acceptance exists. A weakness was discovered before it mattered under external scrutiny.

25.29 Handoff: Who Owns What on Monday?

The implementation provider delivers tenant architecture, administrative-role information, domain and DNS details, identity configuration, Conditional Access design, collaboration settings, device-management configuration, security integrations, migration records, application dependencies, known exceptions, diagrams, and recovery information.

NorthBridge accepts the operational tasks in its service scope. Meridian accepts internal governance and business responsibilities. HarborWatch continues monitoring. Federal Cloud Works moves out of day-to-day operation except for any separately contracted specialist support.

Credentials and administrative access are reviewed. Temporary migration identities and privileges are removed. Documentation owners are assigned.

The project has not ended because the invoice is final. It has ended because permanent operators can explain and maintain the system.

25.30 Internal Readiness Validation

Meridian now conducts a rigorous internal readiness review. The reviewers do not ask teams to present their best examples. They select samples.

A laptop is chosen from inventory and traced across management, EDR, vulnerability, patching, and ownership. A user is selected and traced from authorization to current access. A firewall change is selected and traced from request through verification. A backup is restored. A HarborWatch incident is retrieved. A subcontractor access record is examined.

The reviewers compare policy, SSP, responsibility matrix, technical configuration, interviews, and evidence. Contradictions become remediation items.

This sample-based approach approximates the pressure of assessment more effectively than a rehearsed slideshow.

25.31 The Readiness Review Finds a Documentation Contradiction

An engineer explains that CUI can be printed only on designated devices. The written procedure, however, still contains older language permitting any company-managed printer. The technical and operational practice is more restrictive than the document.

The team determines the approved intended state and updates the procedure. It verifies designated printer configuration and communicates the rule.

The finding demonstrates that documentation can be wrong even when the live practice is stronger. Readiness validation is not only a hunt for weak controls; it is a search for inconsistency.

Assessment credibility depends on one coherent story.

25.32 Preparing People for Assessment Without Giving Them Scripts

Meridian prepares employees by teaching them to explain their own work. Engineering personnel practice describing how they receive and handle protected files. HR explains personnel triggers. NorthBridge explains managed technical functions. HarborWatch prepares to explain its monitoring service if its participation is needed.

The team explicitly tells participants not to guess. If a question belongs to another role, the participant says so and identifies the responsible owner.

Evidence retrieval is practiced, but the organization avoids memorizing canned answers. A scripted answer can collapse when an assessor asks a follow-up question.

Understanding is more durable than rehearsal.

25.33 The Formal Assessment Scenario

For teaching purposes, the remainder of the case now assumes Meridian is pursuing an opportunity for which a Level 2 C3PAO assessment is applicable. This is a hypothetical future/contract-specific scenario used to demonstrate the third-party assessment process; it is not a claim that every Level 2 contractor in September 2026 is currently required to obtain a C3PAO assessment.

Meridian selects an authorized assessment organization through the applicable process and establishes the assessment scope, schedule, participants, and logistics. The readiness specialist does not become the assessor. NorthBridge does not assess its own work. The roles remain distinct.

Meridian provides the requested assessment information and prepares access to evidence and personnel. The company does not create a special assessment-only network. The environment presented is the environment it operates.

The assessment therefore becomes a test of the system built throughout the case study.

25.34 Assessment Opening: Scope Before Controls

The opening discussion confirms the organization, assessment boundary, systems, locations, providers, and key roles. Meridian explains the CUI workflow and target architecture. NorthBridge explains where its managed services intersect the environment.

The assessor asks about the secure file-transfer service and backup provider. Meridian can explain both because external providers were identified during Day-One discovery rather than discovered during assessment.

The assessor also asks why a legacy manufacturing workstation is treated differently. Meridian explains the documented architecture, function, and controls rather than pretending the system does not exist.

Scope discussion establishes the context for everything that follows.

25.35 The First Unexpected Evidence Request

The assessor selects an ordinary user rather than the example Meridian practiced most recently. The team must demonstrate authorization, identity, device relationship, and relevant access.

Meridian's program manager retrieves the business authorization. NorthBridge retrieves identity and device evidence. The records align.

The important point is not that the organization guessed which user would be selected. It is that the same process was used for all users.

Repeatability defeats the fear of random sampling.

25.36 The Assessor Asks About the Missing EDR Agent From Months Ago

Historical evidence includes the rebuilt laptop that temporarily lacked EDR during implementation. Rather than hiding the event, NorthBridge explains how reconciliation found the discrepancy, how the agent was installed, how coverage was verified, and how the endpoint-build procedure was improved.

The event demonstrates control operation. Security did not remain perfect; the organization detected degradation and corrected it.

The assessor can compare the ticket with platform records and the current device state.

This is why Chapter 23 and Chapter 24 emphasized evidence of exception handling rather than only screenshots of healthy dashboards.

25.37 A Live Demonstration Does Not Go as Planned

The assessor asks NorthBridge to demonstrate a particular log query. The technician enters the wrong filter and initially returns no results. The room becomes quiet.

The technician does not invent an explanation. He recognizes the filter error, corrects it, explains what he changed, and retrieves the expected event. The assessor continues with follow-up questions about source health and escalation.

A momentary operator mistake is not automatically the same thing as a failed security requirement. What matters is the actual assessment objective and the evidence available. The team remains factual and lets the assessor evaluate the requirement.

The case teaches a practical lesson: assessment is not theater. Real administrators occasionally mistype commands. Understanding the system matters more than appearing flawless.

25.38 The Provider Interview

HarborWatch participates for the monitoring functions it performs. Its analyst explains log ingestion, detection, investigation, source-health monitoring, escalation, and record retention according to the service.

NorthBridge explains what happens after HarborWatch requests endpoint containment. Meridian explains who owns business and contractual incident decisions.

The three answers connect because the responsibility matrix was built around the actual workflow.

No participant tries to answer the entire incident-response story alone.

25.39 The Subcontractor Evidence Request

The assessor asks how Meridian controls CUI sharing with its machining subcontractor. Contract administration explains authorization and applicable flowdown. Engineering explains what information is shared. NorthBridge demonstrates the approved transfer mechanism and access boundary.

The records show onboarding, authorization, and access. The subcontractor is not given general Meridian network access.

The question crosses contracting, business, and technology. The answer succeeds because the program crosses those functions as well.

This is one of the clearest examples of why CMMC cannot be delegated wholesale to an MSP.

25.40 The Backup Demonstration

The assessor asks about recovery. NorthBridge presents recent backup status, but Meridian does not stop there. It supplies the recovery-test record from the earlier failed exercise and successful retest.

The record shows that the first recovery attempt exposed a missing dependency, the procedure was corrected, and the second attempt restored the service successfully.

That evidence is more educational than a claim that backup has always worked perfectly. It demonstrates a managed process that can identify and correct weakness.

The current runbook is then compared with the tested procedure.

25.41 The Assessment Finding

In this fictional scenario, assume the assessment identifies one requirement that cannot be fully credited based on the evidence available. The team does not argue reflexively. It first makes sure it understands the specific assessment objective and evidence concern.

Meridian determines whether the issue is an implementation gap, evidence gap, documentation inconsistency, or misunderstanding. NorthBridge supplies technical facts. The assessor retains assessment authority.

If the current CMMC rules permit the particular unmet requirement to be placed on a POA&M and the conditions for Conditional status are otherwise met, Meridian follows those rules exactly. The company does not assume every finding is POA&M-eligible.

The remediation receives an owner, technical plan, evidence requirement, and verification method.

25.42 Conditional Status Is Not the Finish Line

Under the current DFARS definition, Conditional Level 2 status is current for no more than 180 days when the applicable conditions are met, and the contractor must successfully close a valid POA&M to achieve Final status. The exact rules in effect at the time of a real assessment must be checked.

In the fictional case, Meridian's remaining item is eligible and is corrected well before the deadline. NorthBridge implements the technical change, Meridian updates the associated procedure and SSP language, and the team performs the required verification.

The applicable closeout process is completed and the record is updated according to the governing requirements.

The lesson is operational: a conditional result creates a time-bounded remediation program, not permission to forget the gap.

25.43 The Final Status and Affirmation Responsibility

Meridian's leadership understands that assessment activity and affirmation are not merely MSP administrative tasks. Current DFARS 252.204-7021 requires annual affirmation of continuous compliance in SPRS for each applicable CMMC UID when the clause applies, and defines current Final Level 2 statuses around a three-year assessment period plus current annual affirmation.

The affirming official therefore needs a reasonable basis for the affirmation. Meridian's operating evidence, provider reviews, changes, incidents, and unresolved exceptions matter.

NorthBridge can supply technical evidence. HarborWatch can supply monitoring evidence. Neither should make the contractor's organizational affirmation on Meridian's behalf unless the legal and regulatory role actually permits and assigns that responsibility.

Accountability remains with the organization required to make the representation.

25.44 The Celebration—and the Warning

Meridian recognizes the achievement. Employees, NorthBridge, HarborWatch, and the project team have done substantial work. Management is entitled to acknowledge the milestone.

The program owner then changes the meeting agenda. The CMMC project meeting becomes the monthly security and readiness review. Open implementation tasks become operational improvement tasks. Provider reviews continue. Access reviews continue. Vulnerabilities continue. Evidence continues.

The warning is simple: the environment will begin changing immediately. Certification or status is not a preservation field around the architecture.

The next test arrives sooner than anyone expects.

25.45 Three Months Later: An Ordinary Tuesday

At 9:17 on a Tuesday morning, NorthBridge's coverage reconciliation reports that an engineering workstation has stopped checking in to the vulnerability platform. RMM and EDR still show the device online.

The technician opens a ticket and investigates. A recent application update changed a local dependency used by the vulnerability agent. The agent service is installed but unhealthy.

NorthBridge repairs the agent and confirms a fresh check-in. The technician runs the expected validation and verifies that the device reappears in the vulnerability population. The ticket records the cause, action, and verification.

No assessor was present. No consultant called Meridian. The program found its own degradation and corrected it.

25.46 The Tuesday Gets More Complicated

Later that day, contract administration informs the program owner that Meridian is considering a new subcontractor for an upcoming package. At almost the same time, Microsoft announces a service change relevant to one of Meridian's integrations.

Neither event is treated as 'an IT issue' alone. The subcontractor enters the contractual and security onboarding process. The Microsoft change enters technical change review. NorthBridge tests the integration. Meridian evaluates business impact. Documentation is updated if the architecture changes.

The same operating model handles a security-agent failure, a business relationship, and a cloud-service change.

This is continuous readiness in practice: different kinds of change enter controlled pathways instead of becoming invisible drift.

25.47 What Meridian Learned About Its MSP

Meridian began the journey believing that NorthBridge either 'handled CMMC' or did not. It ends with a more mature understanding. NorthBridge handles defined technical and operational responsibilities that are essential to Meridian's security program.

The MSP manages systems, implements controls, detects exceptions, performs remediation, preserves records, and supports demonstrations. It also protects its own privileged control planes and technician access.

But Meridian still owns contract understanding, business authorization, provider governance, subcontractor decisions, organizational policies, management risk decisions, and the complete system story.

The relationship becomes stronger because the boundary is clearer.

25.48 What NorthBridge Learned About Serving Defense Contractors

NorthBridge began with a strong general MSP stack. The CMMC engagement forces it to understand that a tool bundle is not a compliance program.

The MSP improves customer separation, technician privilege, evidence retrieval, customer-specific runbooks, provider transparency, escalation, source-health monitoring, and service documentation. It learns to map its services to customer responsibilities without promising that its bundle makes a customer compliant.

It also learns that assessment support is a service discipline. Technicians need to retrieve evidence, explain configurations, and demonstrate operation without improvising claims outside their role.

These improvements benefit other regulated customers as well because they make the MSP more controlled and more transparent.

25.49 What the Readiness Specialist Learned About Operations

The readiness specialist entered the project with knowledge of CMMC requirements and assessment expectations. The engagement reinforces that a correct interpretation is not enough if the technical environment cannot be operated.

Policies must map to tickets. SSP language must map to configuration. Responsibility statements must map to real people. Evidence must be retrievable from systems that actually retain it.

The specialist therefore becomes most valuable when translating requirements into questions that operations can answer and validating whether the resulting implementation is demonstrable.

The specialist does not need to become the MSP. The MSP does not need to become the specialist. The interface between them is where much of the program's quality is created.

25.50 What the Assessor Sees That the Project Team Sometimes Misses

An assessment looks across the complete evidence story. Project teams naturally focus on what they built. The assessor asks whether the implementation satisfies the applicable objectives and whether the evidence demonstrates that fact.

This outside perspective can expose assumptions. A configuration may be technically sophisticated but irrelevant to the requirement being examined. A simple approval record may be critical because it proves authorization. A provider relationship may matter because it performs part of the security function.

The best preparation is therefore not to predict every assessor question. It is to build a coherent environment whose people, technology, documentation, and evidence agree.

Meridian's case succeeds because readiness became an operating discipline before assessment day.

25.51 The Complete Responsibility Chain

The final case can be expressed as a chain. The contract and business determine what must be protected. Meridian determines authorized business use. Architecture determines where the work occurs. Providers perform assigned functions. Technology enforces and monitors portions of the design. People operate the processes. Evidence records what happened. Verification determines whether the outcome is real. Assessment evaluates the applicable requirements. Continuous readiness keeps the system aligned after the milestone.

Breaking any link weakens the story. A requirement without an owner becomes policy language. A technology without an operator becomes shelfware. An operation without evidence becomes difficult to demonstrate. Evidence without verification can document ineffective work. An assessment without continued operation becomes a temporary event.

The chain is the central model of this book.

25.52 Final Case Study Lessons

Meridian did not begin as an irresponsible company. It began as a normal growing contractor whose technology had evolved around business needs. CMMC forced the organization to make security responsibility, architecture, evidence, and provider relationships explicit.

NorthBridge did not begin as an incapable MSP. It began as a capable general MSP whose services had not yet been organized around the evidentiary and responsibility demands of a CMMC customer. The engagement matured the service model.

HarborWatch, Federal Cloud Works, the readiness specialist, subcontractors, and the assessor each played a narrower but important role. None replaced the contractor.

The case demonstrates that successful implementation is not the elimination of every operational problem. It is the creation of a system that knows what should exist, recognizes when reality diverges, assigns the problem, corrects it, verifies the result, and retains evidence.

25.53 Closing the Book: From Readiness to Certification—and Beyond

The title of this book describes a journey from readiness to certification, but the final lesson is that the journey does not end at certification or any other CMMC status. The protected business continues the next morning.

Employees join and leave. Contracts change. New subcontractors appear. Microsoft changes services. Vulnerabilities are published. Security agents fail. Backups need restoration. MSP technicians change roles. Attackers adapt. Evidence ages. Documentation becomes stale unless someone maintains it.

A CMMC-ready organization therefore develops something more durable than an assessment package. It develops an operating discipline in which security, business, contracts, technology, providers, and evidence remain connected.

The contractor cannot outsource accountability, but it can build strong operational partnerships. The MSP cannot become the contractor's entire compliance program, but it can become a disciplined and demonstrable operator of the functions entrusted to it.

CMMC readiness is not demonstrated by the absence of problems. It is demonstrated by an organization's ability to know its environment, protect it deliberately, recognize when something changes or fails, assign responsibility, correct the condition, verify the correction, preserve evidence, and continue operating securely.

That is the destination of the journey, and it is also where the next day of CMMC operations begins.

Regulatory Note for the Case Study

This fictional case deliberately distinguishes the current September 2026 Phase I posture from a hypothetical Level 2 C3PAO scenario used to teach the third-party assessment lifecycle. DoD CIO currently states that Phase II requirements were suspended on July 13, 2026 and that Phase I self-assessment requirements remain in place. Current DFARS 252.204-7021 defines CMMC status, annual affirmation, CMMC UID, flowdown, and Conditional-status requirements. Because CMMC implementation is under review and acquisition requirements can change, a real contractor should verify the solicitation, contract, current DoD CMMC guidance, 32 CFR part 170, current DFARS, and other applicable requirements before relying on any implementation or assessment path described in this educational case.

Current DFARS 252.204-7021 defines current Final Level 1 status as not older than one year with current affirmation, and current Final Level 2 Self or C3PAO status as not older than three years with current annual affirmation. When the clause applies, it also addresses maintaining the required current CMMC status for applicable contractor information systems, flowdown, annual affirmation, CMMC UIDs, and conditional-status POA&M closeout.

Because CMMC implementation is under review and acquisition requirements can change, a real contractor should verify the solicitation, contract, current DoD CMMC guidance, 32 CFR part 170, current DFARS, and other applicable requirements before relying on any implementation or assessment path described in this educational case.

25.54 Going Back Inside the First Executive Meeting

To understand why Meridian's program ultimately works, it is useful to return to the first executive meeting and slow the conversation down. The president wants a binary answer because the business opportunity has a deadline. The operations director wants a project plan. Engineering wants assurance that production will not be disrupted. NorthBridge wants to know what systems are affected. Contract administration wants to know exactly what the prime is requiring. Each person is asking a reasonable question, but none of those questions alone defines the project.

The readiness lead explains that the organization must separate three ideas. The first is contractual applicability: what the solicitation or contract requires. The second is security implementation: what protections the environment actually needs and how they operate. The third is assessment status: how the applicable requirements are demonstrated under the current program rules. Treating those as one question is how organizations buy technology before understanding the problem.

Management therefore authorizes a short discovery phase before approving a major technology purchase. That decision protects both security and budget. The team can still correct obvious urgent weaknesses immediately, but it will not redesign the entire company based on a product salesperson's interpretation of CMMC.

The meeting ends with named decisions rather than vague enthusiasm. Contract administration will produce the governing contract information. Engineering will provide representative workflows. NorthBridge will export inventories and provider dependencies. The readiness lead will organize the requirements-to-evidence model. The operations director will resolve business conflicts and approve resources.

25.55 What the CUI Interview Actually Sounds Like

The interviewer does not begin by asking an engineer to recite the regulatory definition of CUI. Instead, she places a sample project on the screen and asks, 'When this package arrives, what is the first thing you do?' The engineer demonstrates the customer portal. 'Where does it go after you download it?' The engineer shows a local working folder and the engineering share. 'Who else needs it?' The engineer identifies two coworkers and an outside machine shop.

The next question is deliberately practical: 'What happens when the file is too large for the normal method?' That is when the commercial sharing workaround appears. Another engineer adds that he sometimes downloads a drawing to a laptop before traveling because the plant VPN is slow from hotels.

These answers reveal information paths that no network diagram contained. The team now has local storage, remote work, an external sharing service, a subcontractor, and a performance problem influencing user behavior.

The interviewer records the facts without accusing the employees of violating a policy they may never have been taught. The purpose of discovery is to expose the real system. Remediation comes after the organization understands why the real system developed.

25.56 Turning the Interview Into a Data-Flow Diagram

The team converts the conversation into a diagram that begins with the prime's delivery point. Arrows show the drawing reaching a managed endpoint, the engineering repository, the CAD application, backup, approved collaboration, the subcontractor exchange path, and the production output. Administrative paths are drawn separately so the team can see how NorthBridge technicians, security platforms, and cloud administrators reach the systems.

Each arrow receives a question. What information crosses this connection? Is it encrypted as required? Who authorizes the transfer? Which identity is used? Which logs exist? Does an external provider participate? Can the path be disabled? What evidence would prove the design is operating?

That questioning turns a drawing into a security model. A line from a laptop to a file share is no longer decorative. It represents identity, authorization, network connectivity, endpoint state, file permissions, logging, and operational ownership.

When the team cannot answer one of those questions, it marks the diagram with an unresolved item rather than filling the gap with an assumption.

25.57 How the Team Reconciles Four Different Asset Lists

NorthBridge creates a reconciliation worksheet with one row per candidate asset and columns for serial number, hostname, assigned user, business owner, operating system, RMM state, EDR state, vulnerability state, device-management state, backup relevance, location, and disposition. The worksheet is not intended to become another permanent inventory platform. It is a temporary investigative view used to reconcile authoritative systems.

A technician begins with the accounting list because it contains purchase records, then matches RMM by serial number and hostname. EDR and vulnerability exports are joined using stable identifiers where possible. Duplicate hostnames and rebuilt devices are investigated manually.

An asset with RMM but no EDR is not automatically labeled noncompliant. The team asks whether the endpoint should have EDR, whether the record is stale, whether the device is being rebuilt, or whether the agent failed. The disposition determines the corrective action.

The process ends only when every discrepancy has a reason and owner. The reconciled population then informs the permanent inventory and the recurring coverage-reconciliation process.

25.58 How NorthBridge Redesigns Technician Access

NorthBridge's broad senior-engineer group is convenient because any senior technician can solve any customer problem. It is also a large privileged blast radius. The MSP maps its technicians to service duties and identifies who actually needs routine Meridian access.

Four engineers receive customer-specific operational roles. A smaller escalation group can obtain elevated access through the MSP's approved process when necessary. Help-desk personnel retain only the functions required for ordinary support. Emergency access is separately controlled and logged.

The MSP then tests the design. A help-desk technician can reset an authorized user's password but cannot alter tenant-wide security policy. A Meridian engineer can administer the agreed systems but cannot enter another customer's protected documentation through the Meridian role.

NorthBridge documents how temporary escalation works so least privilege does not become an excuse for operational delay. Security and serviceability are designed together.

25.59 The Forgotten Administrator Account: Full Troubleshooting Walkthrough

The obsolete administrator account discovered during readiness is handled as a potential dependency rather than deleted impulsively. NorthBridge first checks sign-in history and administrative activity. It searches automation, application registrations, scheduled tasks, scripts, documentation, and the credential vault for references.

No current dependency is found. The team confirms that the account was created during an earlier migration and retained as a troubleshooting shortcut. Its exclusion from the normal access policy is no longer justified.

A change ticket identifies the account, reason for removal, evidence reviewed, rollback consideration, and approver. NorthBridge disables the account before permanent deletion and monitors for unexpected failures. When none occur, the account is removed according to the approved process.

The team then asks the more important question: could another migration-era account exist? It reviews privileged populations and policy exclusions rather than treating the discovered account as an isolated mistake. The correction therefore improves the system, not just one object.

25.60 What the Backup Failure Looks Like in the Room

During the recovery exercise, the storage data restores successfully. The technician announces that the restore is complete, but the engineering representative attempts to open the recovered application and receives an authentication error. This changes the definition of success immediately.

The team traces the application dependency. The recovered server expects a related identity or service component that was not included in the documented recovery sequence. The data is present, but the business service is not usable.

NorthBridge updates the dependency map, recovery order, and credentials required during restoration. A second test is scheduled using a clean recovery target so the team is not merely continuing from the partially repaired first attempt.

On the retest, an authorized engineering user signs in, opens representative data, saves a controlled change, and confirms the service behaves normally. Meridian records recovery time, issues encountered, corrections, and verification. The evidence demonstrates recoverability rather than backup existence.

25.61 How Meridian Chooses Between Fixing the Enterprise and Building an Enclave

The architecture workshop compares two operating models. In the enclave model, a smaller set of users and devices would handle CUI in a constrained environment. This could reduce the number of systems requiring the same degree of treatment, but it would introduce workflow boundaries that employees must respect every day.

In the broader engineering model, more endpoints and services fall within the controlled environment, increasing management cost. The advantage is that engineers can perform normal work without repeatedly moving files across an enclave boundary.

Meridian tests both ideas against real workflows: engineering collaboration, manufacturing access, remote work, subcontractor exchange, quality records, printing, backup, support, and incident response. The team also considers whether legacy applications can be isolated or must remain connected.

The decision is documented as a business-security tradeoff. Scope is not minimized for its own sake. It is designed so the organization can actually maintain the controls.

25.62 What 'Government Cloud Implementation' Means in the Case Study

Federal Cloud Works begins with tenant and eligibility prerequisites rather than installing a product called GCC High on each laptop. The cloud environment is provisioned and configured; associated client applications, endpoint management, security components, and integrations are then deployed or reconfigured around it.

The implementation sequence covers domains and DNS, identity synchronization or migration strategy where applicable, administrator roles, authentication, access policy, Exchange, collaboration, SharePoint and OneDrive design, Teams where used, device management, Defender capabilities where licensed and selected, application integrations, secure mail and collaboration workflows, and logging.

NorthBridge attends configuration sessions because it will inherit administration. It records not only which settings were chosen but why. A configuration without rationale is harder to maintain when Microsoft changes a service or Meridian adds a requirement.

The implementation team maintains a decision log for features that differ from Meridian's previous environment. If an integration is unavailable or behaves differently, the team identifies an alternative rather than assuming commercial-cloud instructions apply unchanged.

25.63 A Migration Weekend in Detail

Before migration weekend, Meridian freezes nonessential changes. The team confirms user populations, data sets, DNS plans, rollback conditions, support contacts, application test scripts, and communication channels. Engineering identifies the business processes that must work Monday morning.

The migration begins with controlled batches rather than an all-or-nothing leap where feasible. Technicians monitor identity, mail, collaboration, device access, and application behavior. Problems are recorded with timestamps and owners.

One group of users cannot reach an engineering collaboration location after migration. NorthBridge verifies identity and device compliance. Federal Cloud Works checks the cloud-side permission mapping. The cause is an overlooked group-membership translation, not Conditional Access. The mapping is corrected and tested with two users before broad application.

Monday acceptance is based on business scenarios: users can authenticate, reach authorized information, send and receive required communications, use engineering applications, and obtain support. Migration statistics alone do not declare success.

25.64 How Conditional Access Is Tested Instead of Merely Enabled

The team writes test cases before calling the access policy complete. An authorized standard user on a compliant managed device should reach the approved resource. The same user on an unmanaged device should receive the intended restriction. A privileged administrator should encounter the stronger administrative requirements. A disabled user should fail.

NorthBridge records expected and observed behavior. If a test unexpectedly succeeds, the team investigates group membership, exclusions, device state, authentication context, and policy targeting. If a test unexpectedly fails, it examines the same components rather than weakening the policy globally.

Break-glass or emergency access is tested according to its documented purpose without normalizing its routine use. Monitoring must make emergency use visible.

The evidence is not a screenshot of a policy toggle. It is proof that the policy produces the intended business-security outcome.

25.65 How the Endpoint Build Is Proven

NorthBridge selects a clean laptop and performs the build while the project team watches. The technician records the asset, applies firmware and operating-system updates, enrolls management, confirms encryption, installs or validates EDR, connects RMM, establishes vulnerability coverage, applies approved applications, and verifies configuration.

The team then looks at the device from the server side. Does Intune or the selected management platform see it? Does EDR report healthy? Does RMM show the correct customer and policy? Does vulnerability management recognize it? Does the identity platform treat it as expected?

This two-direction verification matters because local installation can appear successful while the cloud service never receives a healthy check-in.

The procedure ends with a business test. The assigned user reaches the authorized engineering resource and cannot reach an unauthorized one. The endpoint is now a functioning component of the architecture, not simply a configured laptop.

25.66 The Firewall Log Failure: Detection to Closure

HarborWatch's source-health logic notices that expected firewall events have stopped. The analyst checks whether the silence is caused by normal maintenance or an ingestion problem. Finding no scheduled maintenance, HarborWatch opens a priority service escalation.

NorthBridge confirms the firewall is online and traffic is flowing. It checks the logging destination, network path, certificate state, and recent configuration changes. The expired certificate is identified.

The technician renews the certificate through the approved change process and generates controlled test events. HarborWatch confirms receipt and verifies timestamps and device identity. The monitoring gap is documented.

The post-event review adds certificate-expiration monitoring and ownership so the same failure is less likely to recur. The event becomes evidence of both detection and improvement.

25.67 A Vulnerability Exception From Beginning to End

The production server with the critical vulnerability supports a manufacturing process that cannot stop during the current run. NorthBridge documents the affected software, vulnerability, exposure, available patch, and required restart.

Meridian operations evaluates the business consequence of immediate downtime. Security evaluates the exposure and possible interim mitigation. Management approves a short exception with a specific maintenance time, owner, and expiration.

NorthBridge applies the mitigation, HarborWatch increases attention to relevant indicators where practical, and the ticket remains open. At the approved window, NorthBridge patches and restarts the server.

Verification follows. The service is tested by the business owner, and vulnerability management confirms the condition is remediated. The exception is formally closed rather than left to expire silently.

25.68 How a Policy Becomes a Procedure and Then Evidence

Consider Meridian's statement that access is removed promptly when employment ends. The policy establishes management intent. The offboarding procedure explains how HR triggers the event, how managers identify special application access, how NorthBridge disables identities, how sessions are revoked, how devices are recovered, and how exceptions are escalated.

When an employee leaves, the HR record and service ticket become evidence of the procedure operating. Identity logs can demonstrate technical action. Application records can demonstrate removal from non-federated systems.

Periodic sampling verifies the process. Meridian selects a former employee and checks whether all expected access is gone. If a forgotten application account is found, the process is corrected.

This layered model—policy, procedure, operation, evidence, verification—is repeated throughout the program.

25.69 How the SSP Is Written Without Becoming Fiction

For each security requirement, the SSP writer asks the operational owner to explain what actually happens. The writer then checks the explanation against architecture and evidence. This prevents polished prose from outrunning reality.

If NorthBridge says it performs vulnerability scanning, the SSP identifies the relevant service and responsibility without claiming that the MSP makes Meridian's business risk decisions. If HarborWatch monitors selected sources, the SSP does not say 'all logs are monitored' unless that statement is true.

Implementation details are written at a level that remains useful after ordinary operational changes. The SSP should not require revision every time a laptop is replaced, but it should change when the architecture, provider, responsibility, or implementation method materially changes.

The document is therefore maintained as a system description, not an assessment script.

25.70 The Evidence Room Before the Assessment

Meridian creates an organized evidence repository with controlled access. Evidence is grouped by requirement or implementation area, but the team avoids duplicating sensitive records unnecessarily. References point to authoritative systems where live demonstration is more appropriate.

Each evidence item has an owner and context. A screenshot without date, system identity, or explanation may be difficult to interpret later. A ticket without the underlying verification may show activity but not outcome.

The team conducts timed retrieval exercises. A reviewer names an employee, device, vulnerability, backup test, or change, and the responsible people locate the supporting record. Slow retrieval exposes documentation or access problems before assessment.

Evidence preparation becomes a test of operational memory.

25.71 The Assessment Opening Meeting in Greater Detail

Meridian's program owner introduces the company, business, assessment boundary, major locations, information flows, and provider relationships. The assessor confirms the scope and explains assessment logistics and communication.

NorthBridge is present for technical areas it operates but does not dominate the opening. Meridian remains the organization being assessed. HarborWatch joins only when its monitoring role becomes relevant.

When the assessor asks who can authorize an engineer's access to a program, NorthBridge does not answer. Meridian's program manager does. When the assessor asks how the authorized account is technically provisioned, NorthBridge explains its process.

The division of answers demonstrates the responsibility model in real time.

25.72 A Full Sample Interview: Access Control

The assessor selects an engineer named Daniel. Meridian produces the manager's authorization showing Daniel's program assignment. NorthBridge locates Daniel's identity and group memberships. The assessor asks why each group is needed.

The program manager explains the business authorization. NorthBridge explains how the group grants technical access. The assessor then asks what would happen if Daniel transferred to a commercial project tomorrow.

Meridian explains the personnel and manager trigger. NorthBridge explains removal. The assessor asks for a previous transfer example, and the team retrieves one.

The conversation moves from a static account screenshot to lifecycle operation. The strongest answer is the process working across time.

25.73 A Full Sample Interview: Vulnerability Management

The assessor asks how Meridian knows which systems need remediation. NorthBridge explains scanning coverage, asset reconciliation, triage, tickets, maintenance, exceptions, and verification.

The assessor selects a historical critical vulnerability. NorthBridge retrieves the original finding and remediation ticket. Meridian explains why downtime was delayed for the production server. The exception record shows approval and expiration.

The assessor then asks how the team knew the patch worked. NorthBridge produces the subsequent verification. The business owner confirms the service was tested after restart.

The evidence chain demonstrates detection, decision, action, and outcome.

25.74 A Full Sample Interview: Incident Response

The assessor asks Meridian what happens when HarborWatch detects suspicious activity after hours. Meridian's incident lead explains the escalation model. HarborWatch explains detection and notification. NorthBridge explains containment authority.

The assessor asks what happens if HarborWatch cannot reach NorthBridge. The current escalation list contains alternate contacts because the tabletop exercise previously exposed that weakness.

The team retrieves the tabletop record showing the failed contact and correction. The exercise itself becomes evidence that the process was tested.

The assessor can see that incident response is not a document stored in a folder; it is a practiced relationship.

25.75 When Evidence Conflicts During Assessment

Suppose a procedure says privileged access is reviewed quarterly, but the latest completed review is four months old. The team should not alter the date or describe the review as current.

Meridian explains the factual condition and provides the available evidence. The assessor determines the consequence against the applicable objective. Internally, Meridian immediately investigates why the recurring task was missed.

The root cause may be that the task was assigned to an employee who changed roles without reassignment. Corrective action therefore includes completing the review and repairing the governance mechanism that schedules and escalates future reviews.

Truthful handling protects the integrity of the assessment and produces a stronger program than cosmetic evidence repair.

25.76 What a Failed Demonstration Should Trigger

When the technician initially enters the wrong log filter, Meridian does not interrupt to coach the answer. The technician corrects the query and explains the mistake.

If the demonstration had failed because the log did not exist, the team would not fabricate a substitute. It would determine whether other evidence satisfies the objective and allow the assessor to evaluate it.

Afterward, Meridian would treat a genuine missing capability as a finding requiring correction. The assessment room is not the place for uncontrolled production changes made simply to create an appearance of compliance.

This discipline separates evidence presentation from emergency engineering.

25.77 How the Fictional Finding Is Remediated

The fictional eligible finding is translated into a remediation plan with a specific technical outcome rather than a vague statement such as 'improve security.' The owner identifies affected systems, implementation steps, test method, evidence, and completion authority.

NorthBridge performs the assigned technical work through change control. Meridian updates documentation where the implementation description changed. The readiness team verifies the correction independently of the technician who performed it.

The closeout evidence is organized so the applicable assessor or process can evaluate the corrected objective under the governing rules.

The team also searches for the same weakness elsewhere. Correcting only the sampled system would leave a systemic problem.

25.78 Why Conditional Status Has Operational Consequences

A Conditional Level 2 status is time-bounded under the current DFARS framework; it is not a relaxed permanent state. Meridian therefore treats the remediation deadline as a management obligation.

The program owner places the item on the executive risk register. NorthBridge places the technical work in its project queue. Evidence and closeout are scheduled from the beginning rather than after implementation.

Weekly review tracks progress and blockers. If a vendor dependency threatens the timeline, management learns early enough to act.

The process demonstrates how regulatory timing becomes ordinary project governance.

25.79 The Affirming Official's Question

Before annual affirmation, the affirming official should not merely ask, 'Did we pass last year?' A more useful question is whether the organization has maintained continuous compliance with the requirements associated with the applicable status and whether material changes or unresolved conditions affect that representation.

Meridian's program owner presents major changes, provider changes, significant incidents, open exceptions, access-review status, vulnerability trends, evidence samples, and documentation updates. NorthBridge and HarborWatch provide their operational inputs.

The affirming official is not expected to personally operate every security tool. The role depends on an organizational process capable of producing a reasonable factual picture.

This is why continuous readiness supports governance as well as assessment.

25.80 The Cost Conversation After the Assessment

Once the project milestone is reached, Meridian reviews recurring cost. Management asks whether every implementation tool must remain. The correct answer is not automatically yes.

The team maps each product back to the security and operational function it performs. If two tools overlap, consolidation may be possible. If a product is removed, the team identifies what capability, evidence, integration, or procedure must replace it.

NorthBridge also reviews service labor. Some recurring manual reconciliation can be automated safely. Other tasks, such as business access authorization, should remain deliberate human decisions.

Cost optimization therefore occurs through architecture and responsibility analysis rather than indiscriminate license cancellation.

25.81 Six Months Later: A New Contract Changes Scope

Meridian wins a new program involving a different engineering application and a new customer portal. Instead of connecting the application immediately, contract administration and the program owner initiate the change review.

The team maps the new information flow, evaluates the application, determines endpoint and server dependencies, reviews provider involvement, and decides whether the existing boundary remains accurate.

NorthBridge tests the application in the controlled environment. HarborWatch determines whether new logs or detections are appropriate. Documentation and diagrams are updated before production use.

The new contract becomes proof that the Chapter 24 implementation model has become repeatable.

25.82 Nine Months Later: NorthBridge Replaces Its RMM Platform

NorthBridge decides to replace its RMM platform across customers. For Meridian, this is not merely an MSP internal tooling decision because the platform provides privileged administration and operational evidence.

The MSP explains the transition, security model, technician roles, integration changes, and timeline. Meridian evaluates the effect on its documented environment and provider responsibilities.

Agents are migrated in controlled groups. During each wave, NorthBridge reconciles old and new populations so no endpoint silently loses management. Privileged access is tested. Automation targeting is validated to prevent cross-customer mistakes.

After migration, old agents, credentials, integrations, and access are removed. Meridian's SSP and provider documentation are updated where needed.

25.83 One Year Later: The Program Reviews Itself

The annual review returns to the same questions asked on Day One. What contracts are active? What FCI and CUI flows exist? Which systems and providers support them? Who performs each responsibility? What changed? What evidence demonstrates operation?

The answers are now produced from an operating program rather than a discovery project. Inventory reconciliation is routine. Provider roles are documented. Access

reviews have history. Backup tests have history. Incident exercises have history. Changes have records.

The review still finds improvements. One diagram contains an old server name. A procedure references a retired ticket field. Two low-risk exceptions have remained open longer than management prefers.

The organization corrects them. Maturity is visible not because the review finds nothing, but because the organization can find, assign, and close discrepancies.

25.84 What Would Have Happened If Meridian Had Bought Tools First?

If Meridian had responded to the original prime-contractor question by purchasing a compliance-branded security bundle, the unapproved file-sharing workflow might have continued. The forgotten administrator account might have survived. The backup dependency might have remained undiscovered. The subcontractor authorization problem would not have been solved by EDR.

The company could have spent substantially more while still lacking a coherent evidence story. Technicians might have operated excellent tools without knowing which business responsibilities they supported.

The case study therefore does not argue against technology. Meridian depends heavily on technology. It argues that technology must be selected and operated inside a defined business, contractual, architectural, and evidentiary model.

Tools become powerful when the organization knows what job each tool is performing.

25.85 What Would Have Happened If Meridian Had Outsourced Everything?

Suppose Meridian had told NorthBridge, 'You own CMMC now.' NorthBridge could have strengthened endpoints and cloud configuration, but it could not truthfully decide which subcontractor should receive CUI, authorize an engineer to a defense program, interpret every contract on Meridian's behalf, or make every management risk decision.

The MSP also could not make Meridian employees follow a secure workflow if the business process made the workflow unusable. Nor could it independently affirm facts that require organizational authority.

Outsourcing technical operation is often practical. Outsourcing specialized advice is often practical. Outsourcing monitoring is often practical. What remains necessary is contractor governance over how those services fit the organization's obligations.

The case succeeds because outsourcing becomes structured delegation rather than abdication.

25.86 What Would Have Happened If Meridian Had Kept Everything Internal?

The opposite extreme is also unnecessary. Meridian does not need to hire a full SOC, cloud migration practice, backup engineering team, and 24-hour help desk merely to prove ownership.

It can use capable providers when responsibilities, access, security, evidence, and escalation are understood. The contractor's accountability is compatible with external performance.

The practical question is therefore not internal versus outsourced. It is whether the organization knows who performs the function, whether the provider relationship satisfies applicable requirements, whether the service can be demonstrated, and whether Meridian governs the result.

This distinction makes CMMC achievable for smaller organizations that could never replicate every specialist capability internally.

25.87 The Case Study as a Reusable Template

A reader can replace Meridian with the reader's own organization and repeat the sequence. Start with the contract and information. Walk the real workflow. Draw the information paths. Reconcile assets. Identify providers. Assign responsibility. Assess gaps. Design architecture. Implement deliberately. Test business outcomes. Build documentation from reality. Generate evidence through operation. Validate by sampling. Prepare people to explain their roles. Maintain the system after the milestone.

An MSP can perform the same substitution with NorthBridge. Decompose the service stack. Protect privileged control planes. Limit technician access. document customer-specific responsibilities. Reconcile coverage. Preserve evidence. Practice escalation. Participate in assessment only for the functions actually performed.

The sequence is intentionally reusable because the technologies will change faster than the underlying operating questions.

The chapter's fictional story therefore becomes an implementation pattern rather than merely a story.

25.88 Final Expanded Perspective: The Book Ends Where Operations Begin

The first question in the case was whether Meridian was 'CMMC compliant.' By the end, Meridian has learned why that question was too small. Compliance status matters, but the organization also needs to know whether the environment can continue protecting the work after people, contracts, software, providers, and threats change.

The strongest evidence of the program is not a binder on assessment day. It is the ordinary Tuesday when a security agent fails and the system notices. It is the employee departure that removes every account. It is the new contract that triggers scope review. It is the MSP platform migration that preserves customer control. It is the annual review that finds stale documentation and corrects it.

That is the operational meaning of readiness. It is a condition continually recreated by governance, technical operation, verification, evidence, and corrective action.

For the defense contractor, the destination is informed accountability. For the MSP, the destination is disciplined service delivery. For both, the enduring objective is a security environment that can explain itself, test itself, correct itself, and continue protecting the mission.

25.89 How Meridian Knows What to Do Next

One of the hardest problems for a first-time contractor is not understanding an individual security requirement. It is knowing what action should follow the discovery of a problem. Meridian solves this by using a repeatable decision sequence rather than depending on one expert to remember everything.

When the team discovers a condition, it first asks what business process and information are affected. It then identifies the applicable requirement or approved architecture, determines who owns the decision, identifies who can perform the technical or procedural correction, defines how success will be tested, and decides what evidence must remain.

This sequence keeps the team from jumping directly from a finding to a product. A missing protection may require configuration, workflow redesign, provider action, policy correction, training, or several of those together.

The sequence also creates a natural handoff. The readiness specialist can identify the requirement. Meridian can make the business decision. NorthBridge can implement its assigned technical change. The evidence owner can preserve proof. No participant needs to pretend to own every discipline.

25.90 The Decision Log: Why It Becomes One of the Most Valuable Records

Meridian maintains a decision log throughout the project because six months later people will remember the outcome but forget why the outcome was chosen. The log records the issue, alternatives considered, responsible decision maker, supporting facts, decision, date, and any condition requiring later review.

The government-cloud choice is one example. The enclave decision is another. The temporary vulnerability exception is another. The log does not replace the SSP or change tickets; it preserves design rationale.

When NorthBridge later replaces its RMM platform, the team can review why particular administrative restrictions were originally chosen. When a new manager asks why engineering cannot use an easier commercial sharing service, Meridian can explain the information and contractual reasoning rather than saying, 'That is just our rule.'

Decision history makes the program maintainable when the original project team is gone.

25.91 The Issue Register: Preventing Unknowns From Disappearing

During discovery, Meridian encounters questions that cannot be answered immediately. Does the CAD integration work in the target environment? Does the subcontractor need a particular status? Who owns a legacy firewall account? How long does a provider retain the needed logs?

Instead of allowing these questions to remain in meeting notes, the project places each one in an issue register with an owner, due date, status, and decision dependency. High-impact unknowns can block architecture approval.

The register distinguishes an unknown from an accepted exception. An unknown means the team does not yet have enough information. An exception means the organization understands the condition and has formally decided how it will be handled.

This simple distinction prevents uncertainty from being converted accidentally into architecture.

25.92 How the Team Determines Whether a Finding Is Technical, Procedural, Documentary, or Governance-Related

When a requirement appears weak, Meridian classifies the cause. If EDR is absent from a required endpoint, the immediate issue is technical. If the endpoint-build procedure never requires EDR verification, there is also a procedural weakness. If the SSP claims all endpoints have EDR when they do not, there is a documentation inconsistency. If nobody owns coverage reconciliation, there is a governance weakness.

One observation can therefore produce several corrective actions. Installing the missing agent fixes today's endpoint but does not prevent tomorrow's recurrence.

The team asks what allowed the condition to exist and what should detect it if it returns. This is the difference between remediation and durable remediation.

Evidence after correction should demonstrate both the immediate fix and, where appropriate, the improved recurring process.

25.93 How Meridian Converts Requirements Into Work Packages

The implementation team does not hand technicians a list of regulatory sentences and tell them to make the network compliant. Each significant requirement is translated into an implementable work package.

A work package identifies the intended outcome, affected systems, prerequisites, responsible implementer, business owner, configuration or procedure changes, test cases, rollback considerations, documentation impact, and evidence expected at completion.

For example, an access-control work package may include group design, privileged-role separation, Conditional Access behavior, application permissions, test users, negative-access tests, logging, and update of the access procedure.

This translation layer lets security requirements enter normal project engineering without losing their original purpose.

25.94 How a Technician Knows When the Work Is Actually Finished

NorthBridge defines completion criteria before implementation begins. A technician does not close an endpoint-enrollment task because the installer returned success. Completion requires the device to appear healthy in the relevant management services and to pass the defined access and security tests.

A firewall logging task is not complete because the firewall says it transmitted logs. HarborWatch must confirm receipt and useful parsing. A backup task is not complete because the job is green. The selected recovery test must succeed.

This approach changes ticket culture. The ticket records outcome verification rather than activity alone.

Where the work changes documentation or recurring responsibility, those follow-up tasks are part of completion rather than optional administrative cleanup.

25.95 How the Program Handles a Control That Cannot Be Implemented as Originally Designed

Projects encounter constraints. A legacy manufacturing system may not support the preferred endpoint agent. An application may require a protocol the target architecture intended to disable. A provider may lack an expected feature.

The team first verifies the limitation rather than accepting 'it cannot be done' as a conclusion. It consults vendor documentation, technical specialists, and controlled testing. If the limitation is real, Meridian returns to the security outcome.

The organization considers redesign, isolation, replacement, compensating measures where applicable, business-process change, or removal of the system from the protected workflow if that can be done legitimately. It does not simply declare the requirement inapplicable because implementation is difficult.

The final decision is documented with ownership and review conditions. If the limitation prevents satisfaction of an applicable requirement, the organization treats that fact honestly under the governing CMMC rules.

25.96 The Difference Between Testing Configuration and Testing Outcome

A configuration test asks whether a setting exists. An outcome test asks whether the setting produces the intended result. Both are useful, but they answer different questions.

NorthBridge can show that MFA is configured for a population. An outcome test attempts the relevant authentication scenario. It can show that a firewall rule exists. An outcome test verifies the prohibited connection fails and the permitted connection succeeds.

Outcome testing often reveals hidden dependencies, exclusions, stale objects, or targeting mistakes that configuration review alone misses.

Meridian therefore combines configuration evidence with representative operational testing.

25.97 How Negative Testing Strengthens the Evidence Story

Security testing should not demonstrate only what an authorized user can do. It should also test what an unauthorized user, unmanaged device, expired account, or disallowed path cannot do when such testing is safe and appropriate.

In the case study, the team verifies that an engineer can reach the assigned project and cannot reach another program. It verifies that an unmanaged device receives the intended restriction. It verifies that a disabled account cannot continue a session according to the designed control behavior.

Negative tests require care because production environments should not be disrupted merely to create evidence. Controlled test identities and systems are useful.

The resulting evidence demonstrates enforcement rather than configuration intent.

25.98 How Meridian Prevents the Evidence Repository From Becoming a Data Dump

The evidence repository has a structure and retention purpose. Meridian does not export every log from every system into a giant folder. That would create cost, security exposure, and retrieval problems.

Instead, the evidence map identifies which authoritative source demonstrates each type of operation and which records should be retained as project or governance artifacts. Live system evidence may be retrieved when appropriate, while key approvals, tests, exceptions, and review records are preserved according to policy.

Sensitive evidence receives access control because evidence itself can contain usernames, architecture, vulnerabilities, administrative details, and other information useful to an attacker.

Periodic retrieval tests confirm that the organization can find what it expects without unnecessarily duplicating the entire environment.

25.99 How Evidence Ages and Becomes Stale

A screenshot showing MFA configuration from nine months ago proves what existed nine months ago, not necessarily what exists today. Meridian therefore considers the time sensitivity of evidence.

Some evidence describes relatively stable architecture. Other evidence must demonstrate recurring operation. Access reviews, vulnerability remediation, backup tests, incident records, and current device coverage naturally change over time.

The evidence map identifies expected refresh or operational cadence rather than treating every artifact as permanent proof.

This is another reason continuous readiness cannot be built from an assessment binder created once.

25.100 How the MSP Prepares Technicians Without Turning Them Into Compliance Consultants

NorthBridge trains technicians on the Meridian service profile. They learn which tools are approved, how privileged access works, what support methods are permitted, which changes require approval, where escalation goes, and how to preserve evidence.

They also learn the boundary of their role. If a customer asks whether a contractual clause applies, the technician does not improvise a legal or compliance interpretation. The technician routes the question to the designated Meridian and readiness contacts.

During an assessment, technicians explain what they perform and demonstrate the systems they operate. They do not claim ownership of Meridian's entire CMMC program.

This role discipline makes technical testimony more credible.

25.101 How Meridian Prepares Employees Who Are Nervous About an Assessor

Employees are told that the objective is accuracy, not performance. They should answer the question asked, describe what they actually do, and avoid guessing.

Training uses normal work examples. An engineer practices showing how a protected file is received and where it is stored. A manager practices explaining how access is authorized. HR practices explaining termination triggers.

If an employee does not know a technical detail, that is acceptable when the detail belongs to NorthBridge. The employee can identify the appropriate role.

Confidence comes from understanding the workflow, not memorizing regulatory vocabulary.

25.102 How the Assessment Team Handles a Request It Cannot Answer Immediately

Not every evidence request will be answered in thirty seconds. Meridian maintains an assessment request tracker recording the request, owner, time received, status, evidence supplied, and any clarification.

If the request is ambiguous, Meridian asks what the assessor needs rather than flooding the room with unrelated documents. If the evidence requires provider assistance, the designated provider contact retrieves it through the agreed process.

The team does not manufacture a new document and present it as historical evidence. Newly created explanatory material is clearly identified for what it is.

The tracker keeps requests from disappearing and helps Meridian learn which evidence was difficult to retrieve.

25.103 How Meridian Responds When the Assessor and Contractor Interpret Something Differently

Meridian first makes sure it understands the question and the assessment objective. It presents the factual implementation and evidence and, where appropriate, the basis for its interpretation.

The organization avoids turning the discussion into a contest. The assessor has an assessment role; Meridian has responsibility to present accurate facts. If a formal

process exists for clarification or dispute, the organization follows that process rather than arguing informally.

After the session, Meridian records the issue and determines whether the disagreement reveals ambiguous documentation or implementation that should be improved regardless of the assessment outcome.

A defensible program benefits from clarity even when the technical control itself was adequate.

25.104 How the Contractor and MSP Should Communicate During an Assessment

Meridian designates who leads each subject. When a question begins with business authorization, Meridian answers first. When it moves into technical provisioning, NorthBridge demonstrates its portion. When monitoring becomes relevant, HarborWatch participates.

Participants avoid contradicting one another by relying on the same responsibility matrix and system description. They also avoid private coaching during testimony that could make an accurate answer look rehearsed or uncertain.

If NorthBridge hears Meridian describe a technical fact incorrectly, it does not embarrass the customer. The team clarifies the fact accurately and professionally.

The goal is one truthful system story told by the people who actually own its parts.

25.105 How a Finding Becomes a Root-Cause Exercise

After any significant finding, Meridian asks why the condition existed. If a review was missed, was the calendar reminder ignored, was ownership lost after a personnel change, or was the review population impossible to obtain? If an endpoint lacked an agent, did the build fail, did the agent break, or did inventory reconciliation fail to notice it?

Root cause does not need to become an elaborate methodology for every minor ticket. It needs to be deep enough to prevent repeated material failures.

Corrective action may therefore change technology, procedure, ownership, training, monitoring, or all of them.

The team verifies not only that the original finding is closed but that the improved process operates.

25.106 How Lessons Learned Feed Back Into the MSP's Standard Service

NorthBridge does not keep every Meridian lesson isolated to one customer. Where appropriate, it improves its standard regulated-customer service.

The missing-agent reconciliation becomes a reusable coverage report. The stale escalation-contact lesson becomes a recurring contact-validation process. The broad technician-role discovery leads to tighter customer-access design. The evidence-retrieval difficulty improves runbooks.

Customer-specific information remains separated, but operational learning can improve the MSP's overall practice.

This is how supporting CMMC customers can mature the MSP without turning the MSP into a certification body.

25.107 How Meridian Knows When a Change Requires CMMC Review

Meridian adds a short security-impact screen to change management. The requester asks whether the change introduces a new CUI flow, provider, privileged path, external connection, location, application, identity model, security tool, or material architectural change.

If the answer is yes, the CMMC program owner or designated security reviewer determines what documentation and validation are needed. Routine endpoint replacement under an unchanged standard build may need no special review beyond normal process.

This prevents two extremes: ignoring security impact entirely and forcing every small IT change through a large compliance committee.

The trigger is material effect on the protected system and responsibility model.

25.108 How New Technology Is Evaluated Before Purchase

When a department requests a new SaaS application, Meridian does not wait until after purchase to ask whether CUI will be placed in it. Procurement asks the requesting owner what information the service will handle, who will access it, what integrations it needs, and whether an existing approved service already performs the function.

Security and contract stakeholders evaluate the provider and intended use according to applicable requirements. NorthBridge evaluates identity, device, logging, administration, and integration impacts.

The decision may approve the service for ordinary business data but prohibit CUI, approve it for the protected workflow, require additional conditions, or reject it.

Procurement becomes a scope-control mechanism rather than merely a purchasing function.

25.109 How AI Tools Enter the Case Study

An engineer asks whether a public generative AI service can help summarize a technical package. Meridian treats the question as an information-handling and provider question, not merely as a new productivity feature.

The organization determines what information would be submitted, how the service handles that information, what contractual and security conditions apply, and whether the service is approved for the intended data. Until the review is complete, employees are instructed not to place protected information into unapproved AI services.

NorthBridge can enforce portions of the policy through technical controls where practical, but Meridian must define acceptable business use and train employees.

The example demonstrates that new technology enters the same governance model as older SaaS: information, provider, authorization, architecture, evidence, and change.

25.110 How Physical Operations Connect Back to the Digital Program

On the manufacturing floor, an engineer prints a controlled drawing for a work activity. The paper leaves the digital environment but not the organization's responsibility.

Meridian's physical procedure defines where protected documents may be printed, how they are controlled during use, where they are stored, and how they are destroyed when no longer needed. The multifunction device itself is included in the technical review because it participates in the workflow.

NorthBridge may secure the device and network connection, but floor supervisors and employees perform the physical handling.

This example reminds the reader that an MSP-centric book must still describe controls the MSP does not own.

25.111 How Remote Work Is Tested as a Complete Scenario

Meridian selects a remote engineer and walks through an ordinary day. The engineer starts a managed laptop, authenticates, reaches approved resources, joins collaboration sessions, receives a technical file, edits it, saves it, and contacts support.

The team checks for local printing, personal cloud synchronization, removable media behavior, home-network assumptions, remote-support methods, and what happens if the laptop is lost.

Where a restriction creates an impractical workflow, the team fixes the workflow rather than relying on employees to tolerate it indefinitely.

Remote work is therefore assessed as a business process, not merely a VPN configuration.

25.112 How Meridian Tests Offboarding as a Negative-Control Exercise

After disabling a controlled test identity, NorthBridge attempts the expected access paths. The test confirms the account cannot sign in and that relevant sessions or tokens behave according to the designed process.

The team checks project groups, specialized applications, remote access, privileged roles, and any direct identities not controlled centrally. Device recovery and data disposition are verified separately.

The purpose is not to attack the environment. It is to confirm that the removal workflow closes the paths the organization believes it closes.

The result becomes both evidence and a test of the application inventory.

25.113 How Provider Failure Is Included in Continuity Planning

Meridian asks what happens if NorthBridge is unavailable during a critical incident, if HarborWatch cannot deliver monitoring, or if a cloud service suffers a significant outage. The answers depend on the service, but the dependencies must be understood.

Emergency contacts, alternate administrative authority, recovery credentials, provider escalation, and business workarounds are documented where appropriate. Meridian does not require itself to reproduce every provider capability internally, but it understands the consequences of provider loss.

Provider continuity is especially important when a single external service holds privileged access or critical recovery data.

Testing selected provider-failure scenarios exposes hidden dependence before an actual outage.

25.114 How the Program Handles Documentation Ownership

Every major document receives an owner responsible for keeping it accurate, not necessarily for writing every sentence. The system owner may own the SSP. NorthBridge may maintain technical runbooks. HR owns personnel procedures. Contract administration owns flowdown records.

Change management identifies documents affected by significant changes. Periodic review checks whether the owner is still the right person.

When an employee leaves, document ownership is reassigned as deliberately as system access.

This prevents the common situation in which an excellent document becomes stale because everyone assumed someone else maintained it.

25.115 How Meridian Handles Exceptions That Keep Getting Renewed

An exception that is renewed repeatedly is treated as a signal. The underlying business or technical problem may require a permanent design decision.

Management reviews the history, cumulative risk, attempted remediation, cost, and alternatives. The organization may fund replacement, redesign the workflow, accept a different documented architecture where permitted, or stop the affected activity.

Renewal is not automatic. Each extension requires current justification and authority.

This keeps temporary conditions from becoming invisible permanent architecture.

25.116 How the Program Distinguishes Metrics From Evidence

Metrics summarize health. Evidence demonstrates specific implementation or operation. Meridian's dashboard may report ninety-eight percent patch compliance, but an assessor or internal reviewer may still ask about a particular server.

The dashboard helps management identify trends and exceptions. The underlying scan, ticket, approval, and verification explain what happened to the selected server.

Good metrics therefore point toward operational evidence rather than replacing it.

The same principle applies to backup success, endpoint coverage, access reviews, incident timing, and training.

25.117 How Management Reads a Monthly CMMC Operations Report

The monthly report begins with material changes and unresolved exceptions rather than pages of green charts. Management sees new contracts, new providers, major architecture changes, security incidents, overdue remediation, failed restore tests, missing security coverage, and upcoming decisions.

NorthBridge explains technical trends in business language. HarborWatch summarizes meaningful monitoring events. Meridian's program owner explains contractual or organizational changes.

Actions are assigned with owners and dates. The next meeting begins by reviewing those actions.

The report therefore becomes a governance mechanism, not a marketing document from the MSP.

25.118 How the MSP Demonstrates Its Own Control of the Customer Environment

Meridian periodically asks NorthBridge to show who currently has privileged access to the customer. The MSP exports or displays the relevant technician roles, temporary elevations, and service identities.

Meridian compares that population with the service model. Unnecessary access is removed. NorthBridge also checks whether departed employees or changed roles have been fully revoked across RMM, vault, documentation, backup, and cloud administration.

The review can sample privileged actions to verify attribution.

This gives the contractor evidence that delegated administration remains controlled after the original implementation.

25.119 How the Case Study Connects Every Provider Without Blurring Accountability

Federal Cloud Works implements specialized cloud changes. NorthBridge operates the managed environment. HarborWatch monitors selected security telemetry. Cloud and backup vendors provide underlying services. The readiness specialist helps organize and validate readiness. The C3PAO, when applicable to the teaching scenario, independently assesses.

Meridian remains the system owner and contracting party responsible for understanding how these relationships fit its obligations. Each provider can be excellent at its function without becoming responsible for every other function.

The responsibility matrix, contracts, SSP, diagrams, escalation paths, and evidence map are the mechanisms that connect the parties.

This is the practical meaning of a shared-responsibility ecosystem.

25.120 The Final End-to-End Test Before Declaring the Case Complete

Before closing the implementation phase, Meridian selects a scenario that crosses the entire environment. A fictional new engineer is hired onto a protected project, receives a managed endpoint, accesses an engineering package, collaborates through the approved method, experiences a simulated security alert, has a file restored, and is then removed from the project.

Each transition is observed. Authorization precedes access. The endpoint appears across expected tools. Monitoring sees the test event. The restore works. Project removal removes access. Evidence is retrievable.

The team records any friction or inconsistency. A failed step returns to the responsible owner for correction and retest.

This exercise proves the architecture as a business system rather than a collection of independent controls.

25.121 Final Teaching Synthesis: What the Reader Should Be Able to Do Tomorrow

After finishing this case study, a contractor should be able to begin with its contracts and information rather than a shopping list. It should know how to convene the right people, walk a real workflow, identify systems and providers, assign responsibility, convert gaps into work, test outcomes, preserve evidence, and establish continuing governance.

An MSP should be able to examine its own stack and determine where it administers, stores, protects, monitors, or can affect the customer's environment. It should know how to control technician access, reconcile coverage, document services, support evidence, participate in assessment, and maintain customer-specific operating procedures.

Neither reader needs to memorize Meridian's architecture. The useful lesson is the reasoning process that produced it.

When the next unknown appears, the organization asks: what information and business process are affected; what requirement or approved design matters; who owns the decision; who performs the work; how will we test the outcome; what evidence will remain; and who will maintain it afterward?

25.122 Final Closing: The Assessment Is a Milestone; the Operating Model Is the Achievement

Meridian's fictional journey began with an executive asking for a yes-or-no answer. The organization eventually learned that the durable answer is a system of responsibilities and operations.

The contract defined the need. Information flows defined the problem. Scope bounded the environment. Architecture connected the technology. Providers supplied specialized capability. Procedures turned policy into action. Evidence made action visible. Testing challenged assumptions. Assessment examined the result. Continuous operations kept the result alive.

The final measure of the program is not whether Meridian can stage a convincing assessment day. It is whether the company and its providers can operate correctly when nobody is watching.

That is why the book ends after the assessment rather than at it. The assessment is a milestone. The operating model is the achievement.

Appendix A

CMMC Readiness Checklist

A Detailed Contractor–MSP Readiness and Evidence Workbook
CMMC for MSPs: From Readiness to Certification
Authored by Dr. Charles Edwards

A.1 Purpose of This Appendix

This appendix is designed to be used, not merely read. It gives a defense contractor and its MSP a disciplined way to determine whether the organization understands its CMMC obligations, has defined the environment that performs the work, has assigned responsibility, has implemented the required protections, and can produce evidence that the protections operate. The checklist should be treated as a readiness-management tool rather than as a substitute for the applicable regulation, contract, assessment guide, or professional judgment.

A check mark should never mean that someone remembers discussing the subject. It should mean that the organization can identify the owner, describe the implementation, demonstrate the operation, and locate appropriate evidence. Where one of those elements is missing, the item should remain open or be marked for investigation.

The checklist deliberately includes contractor and MSP questions side by side. A contractor cannot outsource organizational accountability simply by hiring an MSP. At the same time, an MSP may perform critical security functions whose implementation and evidence materially affect the contractor's ability to demonstrate its environment.

A.2 Current Regulatory Context for Using the Checklist

As of September 2026, DoD states that CMMC implementation is paused in Phase I after the July 13, 2026 suspension of planned Phase II requirements. The current DoD CMMC page describes Level 1 as an annual self-assessment with annual affirmation and Level 2 under the Phase I posture as a self-assessment every three years with annual affirmation. DoD also states that Level 1 POA&Ms are not permitted and that limited Level 2 POA&M use is subject to the governing rules and 180-day closeout requirements. Because implementation rules and contract requirements can change, users of this appendix should always verify the current solicitation, contract, 32 CFR part 170, DFARS, and DoD CMMC guidance before relying on a checklist result.

Current DFARS 252.204-7021 requires, when the clause applies, a current CMMC status at the level specified in the contract for relevant contractor information systems, annual affirmation in SPRS, applicable flowdown to subcontractors and suppliers, and closeout of a valid POA&M when Conditional status applies. A readiness checklist therefore has to include contract administration, information systems, subcontractors, evidence, and continuing affirmation rather than focusing only on endpoint security.

A.3 How to Score Readiness Without Creating a False Compliance Score

This workbook does not assign an unofficial CMMC percentage. A high percentage of checked boxes can conceal one serious unresolved requirement. Instead, each item should receive one of five operational states: Verified, Implemented but Evidence Weak, Partially Implemented, Not Implemented, or Not Yet Determined. 'Not Applicable' should be used only when the organization has a defensible basis for that conclusion.

For every item marked Verified, the reviewer should be able to answer four questions: Who owns the decision? Who performs the work? What evidence proves the outcome? When was it last verified? This turns readiness into an evidence-based operating condition.

A.4 Readiness Status Definitions

Status	Meaning	Required Next Action
Verified	Implementation is understood, operating, tested where appropriate, and supported by evidence.	Maintain; sample again on defined cadence.
Implemented / Evidence Weak	The activity appears to operate, but evidence is incomplete, stale, difficult to retrieve, or poorly contextualized.	Strengthen evidence and perform retrieval test.
Partially Implemented	Some required elements operate, but coverage, workflow, responsibility, or validation is incomplete.	Create remediation work package and retest.
Not Implemented	Required capability or process is absent.	Assign owner, design implementation, execute, verify.
Not Yet Determined	The team lacks enough information to make a defensible conclusion.	Investigate; do not convert uncertainty into an assumption.
Not Applicable	The item does not apply to the defined environment and the basis is documented.	Retain rationale and re-evaluate after material changes.

A.5 Governance, Contract, and CMMC Applicability

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action

Has contract administration identified the solicitations, contracts, task orders, delivery orders, and flowdowns that drive the organization's CMMC obligations?				
Has the organization identified the CMMC level and assessment type actually required by each applicable contractual instrument rather than assuming all defense work has the same requirement?				
Has an affirming official been identified where required, with a process for giving that official current factual information?				
Does the organization know which CMMC UID or contractor information system corresponds to applicable work where required?				
Is there a process for reviewing new opportunities before protected information is accepted?				
Are subcontractor and supplier flowdown decisions owned by contract administration rather than delegated informally to IT?				
Can management explain the difference between contractual applicability, technical implementation, and assessment status?				

A.6 FCI and CUI Discovery

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Has the organization identified where FCI enters, is created, processed, stored, transmitted, printed, backed up, archived, and destroyed?				
Has the organization identified where CUI enters, is created, processed, stored, transmitted, printed, backed up, archived, and destroyed?				
Have real employees demonstrated representative workflows rather than relying only on diagrams or policy statements?				
Have workarounds such as personal email, consumer file sharing, removable media, local downloads, public AI services, and unapproved SaaS been investigated?				
Are business owners able to distinguish ordinary corporate information from FCI/CUI sufficiently to follow approved handling procedures?				
Is there a process for evaluating a new information type or contract when classification/handling is uncertain?				

A.7 Scope and Information Flows

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Is there a current boundary diagram showing systems, networks, cloud services, remote users, administrative paths, external providers, and important information flows?				
Can the organization explain why each major system is in scope, out of scope, a security protection asset, specialized asset, or otherwise treated according to the applicable scoping guidance?				
Do diagrams include backup, monitoring, RMM, identity, collaboration, printers where relevant, and external exchange paths?				
Have remote work and physical CUI workflows been included?				
Does a material change trigger a scope review?				
Can the contractor and MSP tell the same scope story without contradicting one another?				

A.8 Asset and Software Inventory

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Is there an authoritative inventory for endpoints, servers, network devices, virtual systems, cloud resources, and other relevant assets?				
Have RMM, EDR, vulnerability, device-management, and accounting inventories been reconciled rather than assumed to match?				
Are stale, retired, rebuilt, and duplicate device records resolved?				
Is required software and major SaaS inventoried with owner, purpose, and relevant data handling?				
Are legacy and specialized assets explicitly addressed rather than silently omitted?				
Is there a recurring coverage-reconciliation process capable of detecting a device that loses an expected security agent?				

A.9 External Service Providers and MSP Dependencies

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action

Has every relevant ESP been identified, including MSP/MSSP, CSP, backup, SOC/SIEM, cloud, RMM, vulnerability, security, and specialized support providers?				
Does the organization know which providers process, store, transmit, secure, administer, monitor, or can otherwise affect FCI/CUI systems?				
Are applicable provider relationships and responsibilities documented in the SSP or associated responsibility documentation?				
Are provider privileged-access paths known and controlled?				
Are subcontracted MSP functions visible to the contractor rather than hidden behind the primary MSP label?				
Does the contractor understand what happens if a critical provider becomes unavailable?				

A.10 Responsibility Matrix

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	**Status**	**Owner**	**Evidence / Source**	**Last Verified / Action**
Does every important security function have a named organizational owner and operational performer?				

Does the matrix distinguish contractor responsibility, MSP responsibility, shared responsibility, and other-provider responsibility?				
Does each shared responsibility describe the handoff instead of simply saying 'shared'?				
Are approver, performer, evidence owner, escalation owner, and maintenance cadence identified where useful?				
Do service agreements and actual operations align with the matrix?				
Is the matrix reviewed after provider, personnel, architectural, or contractual change?				

A.11 Identity, Authentication, and Privileged Access

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	**Status**	**Owner**	**Evidence / Source**	**Last Verified / Action**
Are ordinary and privileged identities controlled according to the approved design?				
Is MFA implemented and tested for the applicable populations?				
Are Conditional Access or equivalent access policies tested for both permitted and denied scenarios where used?				
Are emergency-access identities deliberately designed, protected, monitored, and				

periodically reviewed?				
Are shared administrator accounts eliminated or tightly justified and controlled where technically unavoidable?				
Are service accounts, API identities, application registrations, and non-human credentials inventoried and owned?				
Can the MSP demonstrate which technicians currently have privileged access to the customer?				
Are technician departures and role changes revoked across RMM, vaults, cloud administration, backup, documentation, and security tools?				

A.12 Endpoint and Device Security

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	**Status**	**Owner**	**Evidence / Source**	**Last Verified / Action**
Is there a defined controlled-endpoint build or baseline?				
Are encryption, EDR, RMM, vulnerability management, patching, device management, and approved applications verified rather than merely installed?				
Does the organization test that an endpoint appears healthy in the authoritative management platforms?				

Are unmanaged or noncompliant device behaviors tested against access policy where appropriate?				
Are mobile devices, removable media, printers, scanners, and specialized devices addressed according to their actual use?				
Can a rebuilt or replacement endpoint be provisioned consistently by someone other than the original implementation engineer?				

A.13 Network, Remote Access, and Segmentation

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Are network segments and permitted paths documented?				
Are legacy remote-access accounts and vendor connections periodically reviewed?				
Does third-party remote access require sponsor, purpose, authorization, and removal/expiration?				
Are remote workers provided an approved workflow that does not encourage local or consumer-service workarounds?				
Are firewall and network changes controlled and evidenced?				

Can the organization demonstrate that prohibited paths fail and approved paths work where safe negative testing is appropriate?				

A.14 Cloud, Microsoft 365 Government, and Collaboration

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Has the organization selected its cloud environment based on actual contractual, data, eligibility, service, and integration requirements rather than a generic 'CMMC compliant cloud' claim?				
Where GCC or GCC High is used, are tenant, identity, roles, access, Exchange, SharePoint, OneDrive, Teams, device management, security, logging, and integrations documented and operationally owned?				
Have application and API compatibility differences been tested?				
Are secure collaboration and file-transfer workflows usable for real business-sized files and external recipients?				
Can permanent operators administer the environment without depending on the implementation provider?				
Has an Operational Acceptance Test				

demonstrated onboarding, access, endpoint enrollment, security monitoring, evidence retrieval, disabling, and recovery?				

A.15 Vulnerability, Configuration, and Patch Management

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Is vulnerability scanning coverage reconciled against the asset population?				
Are findings triaged using severity plus business and exposure context?				
Do remediation tickets show detection, decision, action, and verification?				
Are patch windows defined and are exceptions authorized, time-bounded, and closed?				
Are configuration baselines or approved standards defined for important systems?				
Does emergency change management preserve approval, validation, and documentation?				
Are repeatedly renewed exceptions escalated for permanent architectural or business resolution?				

A.16 Logging, Monitoring, and Security Operations

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Has the organization identified which log sources are required for its monitoring design?				
Is log-source health monitored so silence is distinguishable from absence of malicious activity?				
Are identity, endpoint, network, cloud, and other relevant sources integrated as designed?				
Are alert escalation paths current and tested?				
Can the SOC/MSSP explain what it monitors, what it does not monitor, retention, escalation, and handoff?				
Can the MSP demonstrate what happens after the SOC requests containment or investigation?				
Are monitoring records retrievable as evidence without exposing unnecessary sensitive data?				

A.17 Backup, Recovery, and Continuity

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action

Are backup jobs monitored and failures assigned?				
Has the organization tested restoration of representative business services rather than only individual files?				
Do recovery procedures include application, identity, dependency, credential, and network requirements?				
Are backups protected from the same failure or attack that could affect production where required by the design?				
Are recovery tests documented with failures, corrections, retesting, and business validation?				
Are critical external-provider outages included in continuity thinking?				

A.18 Incident Response

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Are detection, validation, escalation, containment, eradication, recovery, reporting evaluation, and lessons learned assigned to specific roles?				
Do contractor, MSP, SOC/MSSP, legal/contract personnel, and other providers understand their				

handoffs?				
Are after-hours contacts current?				
Has the organization run a tabletop or operational exercise?				
Can the MSP isolate an affected endpoint through the approved process?				
Does the contractor know who makes contractual and organizational reporting decisions?				
Are incident records preserved and used to improve procedures and controls?				

A.19 Personnel, Training, and Physical Handling

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	**Status**	**Owner**	**Evidence / Source**	**Last Verified / Action**
Do onboarding and offboarding connect HR triggers to technical access?				
Are transfers and project changes treated as access-change events?				
Are specialized application accounts included in offboarding?				
Is training scenario-based enough that employees know what to do when the approved method is inconvenient?				
Are physical CUI printing, storage, transport, and destruction addressed				

where applicable?				
Are employees taught what to do when they are uncertain rather than encouraged to guess?				

A.20 Policies, Procedures, SSP, and Documentation

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Do policies describe management intent that the organization can actually perform?				
Do procedures explain who performs the work, when, using what system, with what escalation, and what record remains?				
Does the SSP describe the live architecture and actual provider relationships?				
Are documentation statements reconciled against technical demonstrations?				
Does every major document have an owner?				
Does change management identify documentation affected by material changes?				
Are stale diagrams, retired server names, obsolete contacts, and old provider references corrected through periodic review?				

A.21 Evidence Readiness

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Is there an evidence matrix mapping implementation claims to authoritative evidence sources?				
Does each important evidence type have an owner?				
Can evidence be retrieved within a reasonable period by the people expected to retrieve it?				
Is evidence contextualized with system, date, owner, and purpose rather than stored as unexplained screenshots?				
Is sensitive evidence protected?				
Does the organization distinguish stable architecture evidence from recurring operational evidence?				
Are evidence samples refreshed so the repository does not become an assessment-time snapshot?				

A.22 Assessment Preparation

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified /

				Action
Has scope been internally challenged before assessment?				
Have reviewers selected random samples rather than only the organization's best examples?				
Can employees explain their own work without memorized scripts?				
Can MSP and provider personnel explain only the functions they actually perform?				
Is there an assessment request tracker for evidence requests and follow-up?				
Have live demonstrations been practiced using ordinary operators?				
Does the organization know how it will respond factually if a demonstration or evidence request does not go as expected?				
Are assessor and readiness/consulting roles kept appropriately separate?				

A.23 POA&M and Remediation Governance

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Does the organization understand that Level 1 POA&Ms are not permitted under the current DoD Phase I				

description?				
For Level 2, does the organization verify that any proposed POA&M item is eligible under the governing rules rather than assuming every unmet requirement can be deferred?				
Does every remediation item identify root cause, owner, milestones, dependencies, target date, validation, evidence, and closeout authority?				
Are Conditional-status deadlines tracked at management level where applicable?				
Does remediation search for systemic recurrence rather than fixing only the sampled device or user?				

A.24 SPRS, Status, Affirmation, and Continuing Governance

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	Status	Owner	Evidence / Source	Last Verified / Action
Are required assessment results and CMMC UID information managed in SPRS by authorized personnel where applicable?				
Is annual affirmation tracked as a governance obligation rather than a calendar reminder with no supporting review?				
Before affirmation, does management review material changes, unresolved exceptions,				

provider changes, significant incidents, and current evidence?				
Are status expiration and reassessment timelines monitored?				
Are subcontractor/supplier status and affirmation obligations addressed before award where the applicable clause requires them?				
Does management understand that a prior assessment does not freeze the environment or excuse later drift?				

A.25 Continuous Readiness

Use the following questions as evidence-based review prompts. For each item, record the status, owner, evidence source, last verification date, and corrective action if needed.

Readiness Question	**Status**	**Owner**	**Evidence / Source**	**Last Verified / Action**
Is there a daily/weekly/monthly/quarterly/annual operating rhythm appropriate to the organization?				
Are missing agents, stale accounts, failed backups, absent logs, overdue vulnerabilities, and expired exceptions detected through recurring processes?				
Do new contracts, applications, SaaS services, AI tools, providers, integrations, and remote-work changes enter a security-impact review?				
Are privileged MSP access and provider				

responsibilities periodically revalidated?				
Are restore tests, incident exercises, evidence samples, access reviews, and documentation reviews recurring?				
Can the organization explain what changed since the last assessment or affirmation and how the change was governed?				

A.26 Management Readiness Summary

After completing the detailed sections, management should summarize the unresolved conditions rather than reducing the workbook to a percentage. The most useful summary identifies conditions that could affect contractual eligibility, CUI protection, assessment status, scope accuracy, provider dependence, or the organization's ability to make a truthful affirmation.

Priority Condition	**Business/CMMC Impact**	**Owner**	**Required Action**	**Target Date**	**Verification / Closure Evidence**

A.27 Final Readiness Questions for the Contractor

Before declaring itself ready, the contractor should be able to explain what work drives CMMC, where FCI and CUI exist, what systems and providers are involved, who owns each responsibility, what evidence demonstrates implementation, what material exceptions remain, and how the environment will continue operating after the readiness project ends. If the organization can answer those questions only when a consultant is in the room, the program is not yet operationally mature.

A.28 Final Readiness Questions for the MSP

The MSP should be able to explain exactly which customer functions it performs, which privileged platforms and technicians can affect the environment, how it protects those access paths, how it detects missing security coverage, how it escalates incidents and exceptions, what evidence it can provide, and what responsibilities remain with the contractor or other providers. The MSP should never need to claim that its tool stack makes the customer compliant in order to demonstrate its value.

A.29 Using This Checklist After the Assessment

This appendix should not be archived after an assessment. The same questions can be sampled throughout the year. A mature organization will find occasional discrepancies because environments change. The important operational capability is to detect the discrepancy, assign it, correct it, verify the result, preserve the evidence, and determine whether documentation or architecture must also change.

The checklist therefore supports the central operating principle of this book: readiness is not a one-time condition created for an assessor. It is the continuing alignment of contracts, information, people, technology, providers, documentation, evidence, and management responsibility.

A.30 The CMMC Multi-Party Readiness Model

CMMC readiness becomes much easier to understand when the reader stops treating it as a conversation between one company and one assessor. A defense contractor or offeror normally operates inside a chain of business, technical, compliance, and assessment relationships. The organization seeking or performing the DoD work remains responsible for understanding the contractual requirement and for the contractor information systems used to perform that work. It may, however, depend on an MSP, MSSP, cloud provider, specialized implementation company, backup provider, SOC, subcontractors, suppliers, and readiness professionals.

For practical teaching, this appendix uses three principal operating parties and then separates the independent assessment role. Party One is the Defense Contractor or Offeror: the company that holds the DoD contract or wants to compete for one. Party Two is the MSP/ESP side: the company or companies that implement or operate assigned technology and security functions. Party Three is the CMMC readiness/compliance specialist: the party helping the contractor understand requirements, scope, documentation, evidence, remediation, and preparation. The C3PAO, when a Level 2 C3PAO assessment is required, is intentionally shown separately because an independent assessor is not the contractor's implementation team.

This distinction prevents a common terminology error. A contractor seeking a Level 2 (C3PAO) status is not the same thing as a C3PAO. The contractor is the organization being assessed. The C3PAO is the authorized assessment organization. Similarly, an MSP may materially affect the contractor's CMMC environment without becoming the owner of the contractor's entire CMMC program.

A.31 The Five Questions That Follow Every Responsibility

For each major requirement or operational function, the readiness team should identify five different answers: Who owns the organizational decision? Who implements the capability? Who operates and maintains it after implementation? Who produces or preserves the evidence? Who independently assesses it when an independent assessment is applicable?

Sometimes one organization fills several of these roles. For example, an MSP may implement endpoint protection, operate it every day, and provide evidence. The contractor still owns the business decision to authorize the MSP and remains responsible for understanding how that service supports its environment. The assessor remains independent of those operational roles.

Function	Decision Owner	Implements	Operates/ Maintains	Evidence Provider	Independent Assessment
CUI handling workflow	Contractor/Offeror	Contractor + assigned providers	Contractor + MSP as assigned	Contractor + providers	C3PAO when required
Microsoft/cloud architecture	Contractor approves	MSP or specialized implementer	MSP/internal IT	MSP + contractor	C3PAO when required
Endpoint security	Contractor approves standard	MSP/internal IT	MSP/internal IT	MSP + contractor	C3PAO when required
SSP	Contractor/system owner	Contractor with readiness and technical input	Contractor owns updates	All performers supply facts/evidence	Assessor examines
Assessment readiness	Contractor owns readiness decision	Readiness specialist assists	Contractor maintains	Contractor + providers	Separate from implementation
CMMC assessment	Contractor participates	Not an implementation activity	N/A	Contractor + providers present evidence	C3PAO for Level 2 C3PAO

A.32 Scenario One: The Existing DoD Contractor

The first pathway begins with a company that already performs DoD work. This organization may already receive FCI or CUI, may already have DFARS obligations, may have an SSP and SPRS history, and may have accumulated years of technology decisions. Its problem is not designing a theoretical clean environment. Its problem is determining what actually exists today and whether the contractual, technical, documentary, and evidence stories agree.

The readiness team begins with current contracts and flowdowns, then traces actual FCI/CUI workflows. The MSP demonstrates the systems it operates. The readiness specialist helps reconcile contractual and CMMC requirements with the live environment. Unknown systems, old administrator accounts, consumer sharing practices, legacy remote access, subcontractor flows, missing agents, stale documentation, and provider dependencies are treated as facts to investigate rather than embarrassing details to hide.

For an existing contractor, the most important question is often not 'What should our architecture look like?' but 'What architecture are we already using to perform the contract, and can we defend every material part of it?'

A.33 Scenario Two: The Prospective DoD Contractor or Offeror

The second pathway begins before contract award. A company sees a DoD opportunity and learns that the solicitation specifies a CMMC requirement. Current DFARS 252.204-7025 provides for the solicitation to identify Level 1 (Self), Level 2 (Self), Level 2 (C3PAO), or Level 3 (DIBCAC), and requires the specified current

status or higher before award for contractor information systems that will process, store, or transmit FCI or CUI during contract performance.

The prospective contractor should therefore resist the temptation to say simply, 'We need CMMC Level 2 certification.' The first question is what the solicitation actually requires. Level 2 (Self) and Level 2 (C3PAO) are different assessment paths. The technical protection goals may overlap substantially, but the required status and assessment mechanism must come from the applicable requirement rather than from sales language.

Because the company may not yet possess the future contract's CUI, it has an opportunity to design deliberately. It can define the intended protected workflow, choose the boundary, select providers, establish identity and endpoint standards, build approved collaboration, create the SSP, implement procedures, generate operating evidence, and validate the environment before protected contract work begins.

Readiness before award does not mean inventing evidence for operations that have never occurred. The organization establishes and operates representative processes sufficiently to demonstrate the implemented environment truthfully. Evidence should describe what actually exists and operates, not what management hopes will exist after award.

A.34 Prospective Contractor Readiness Gate

Gate	Contractor / Offeror Question	MSP / ESP Question	Readiness Specialist Question	Evidence / Decision
Solicitation	What CMMC level/status is actually required?	What technical impact does that requirement create?	Has the requirement been interpreted and documented appropriately?	Solicitation/provision review
Information	What FCI/CUI is expected and what work will create/use it?	Which systems/services will touch or protect it?	Is the information-flow assumption complete?	Data-flow narrative/diagram
Boundary	What environment will perform the work?	Which MSP tools/admin paths affect that environment?	Does the scope follow current guidance?	Scope diagram/inventory
Architecture	What design will management approve?	Can the MSP implement and maintain it?	Does design support the requirements without relying on undocumented assumptions?	Architecture decision record
Implementation	Has the approved design been built?	Can technicians demonstrate operation?	Are gaps tracked and resolved?	Tickets/configuration/tests
Evidence	Can the company prove operation?	Can MSP retrieve assigned evidence?	Is evidence sufficient, current, and contextualized?	Evidence matrix
Assessment	Is the required assessment path ready?	Are MSP personnel ready to demonstrate assigned	Has readiness support remained distinct from	Readiness review

		functions?	independent assessment?	
Award/Operation	Is required current status/affirmation available where applicable?	Can MSP support production from day one?	Are unresolved conditions visible to management?	SPRS/status records and operational handoff

A.35 Party One: Defense Contractor or Offeror

The contractor or offeror is the center of the model because it is pursuing or performing the Government work. It owns contract review, business authorization, information handling decisions, provider selection, system ownership, organizational policies, and the truthfulness of representations and affirmations made on its behalf.

The contractor does not need to perform every technical task internally. It can contract with an MSP for identity administration, endpoints, network management, backup, monitoring, vulnerability management, and other services. Outsourcing performance does not eliminate the need to understand what was outsourced, how it is controlled, and what evidence demonstrates the result.

Management should therefore be able to describe its environment without saying, 'Ask our MSP; they handle CMMC.' The MSP can answer technical questions, but the contractor must understand the operating model it has authorized.

A.36 Party Two: MSP, MSSP, and External Service Providers

The MSP's CMMC significance depends on what it actually does and what data or security functions its systems handle. Current DoD Level 2 scoping guidance addresses External Service Providers and states that an ESP can be within the organization's scope when it meets the relevant CUI Asset and/or Security Protection Asset criteria. The guidance also emphasizes documenting the provider relationship and services in the SSP and using the provider's service description and customer responsibility matrix to understand responsibilities.

The practical lesson is that the contractor should not classify every vendor as 'our MSP' and stop there. The team examines RMM, PSA, credential vault, backup, EDR, vulnerability platform, SIEM/SOC, cloud administration, documentation systems, remote-support paths, technician identities, integrations, and subcontracted services. It asks what information resides there, what security protection data resides there, what privileged action is possible, and what service the provider performs.

The MSP should likewise know which of its own systems and people participate in the customer's service. A technician who can administer the protected tenant is not operationally equivalent to a salesperson who cannot access customer systems.

A.37 Party Three: The CMMC Readiness and Compliance Specialist

The readiness specialist helps turn requirements into an organized readiness program. This role may facilitate scoping workshops, responsibility mapping, gap analysis, SSP development, evidence mapping, remediation tracking, management education, mock interviews, and internal readiness validation.

The specialist should not become a substitute for the contractor's management or for the MSP's technical operators. A consultant can help write an accurate SSP, but the contractor and technical providers must supply the facts. A consultant can recommend a remediation approach, but authorized system owners must approve changes and qualified operators must implement them.

The strongest readiness specialist therefore makes the organization less dependent on the specialist over time. By assessment time, Meridian-like organizations in this book should be able to explain and operate their own environment.

A.38 The C3PAO: Why the Assessment Role Must Remain Distinct

When the solicitation or contract requires Level 2 (C3PAO), the C3PAO performs the independent assessment role. The assessment organization is not simply the fourth member of the implementation project team. The contractor, MSP, and readiness personnel prepare and operate the environment; the C3PAO evaluates the applicable assessment scope and evidence according to the governing CMMC assessment process.

During assessment, the MSP may participate because it performs relevant technical functions. The readiness specialist may help the contractor organize beforehand. Neither fact transfers contractor accountability to those parties.

This distinction should appear throughout the book because the words consultant, assessor, MSP, ESP, and C3PAO are not interchangeable.

A.39 Supporting Parties: Specialized Implementers, CSPs, SOCs, Backup Providers, and SaaS

Many real implementations contain more than three operational organizations. A specialized Microsoft Government cloud provider may perform a tenant migration and then hand operations to the MSP. A CSP may supply licensing or cloud services. A SOC may monitor security telemetry. A backup provider may hold protected backups or security-relevant configuration. A SaaS provider may participate in a protected workflow.

For each supporting provider, the contractor repeats the same analysis: what service is provided; what information or security protection data is involved; what privileged capability exists; what responsibilities belong to the provider and customer; what evidence is available; what happens when the service changes; and what happens when the relationship ends.

The result is not a flat vendor list. It is a service-dependency map connected to scope, responsibility, evidence, and continuity.

A.40 Prime Contractor, Subcontractor, and Supplier Flowdown

The multi-party model also extends down the supply chain. Current DFARS 252.204-7021 requires the contractor to flow the appropriate CMMC requirements to applicable subcontracts and other contractual instruments and, before subcontract award, to ensure the subcontractor has the appropriate current CMMC certificate or status for the information being flowed down.

The prime contractor therefore needs a repeatable decision process before sending FCI or CUI to another company. What information will the subcontractor receive? What level applies? Which subcontractor systems will process, store, or transmit it? Has the required status and affirmation been verified where applicable? What contract language and incident/escalation obligations must flow down?

The MSP can help establish secure exchange and access, but the prime contractor's contracts and supply-chain functions own the business decision to release information and award the subcontract.

A.41 A Three-Party Responsibility Workshop

The responsibility workshop should place the contractor, MSP, and readiness specialist in the same room. For each security function, the group begins with the contractor's required outcome. It then identifies the actual technical or procedural implementation, the operating owner, the evidence source, and any external dependency.

If the MSP says it patches servers but the contractor assumes the MSP also patches an engineering application, the difference is documented immediately. If the readiness specialist expects ninety days of a log source but the SOC contract provides less, the team identifies the gap before assessment. If the contractor believes the cloud implementer will maintain the tenant indefinitely but the statement of work ends after migration, the handoff problem is exposed.

The workshop succeeds when every participant can describe not merely its own responsibility but the handoff to the next participant.

A.42 Multi-Party Responsibility Matrix

Activity	Contractor / Offeror	MSP / ESP	Readiness Specialist	Other Provider	C3PAO When Applicable
Contract/CMMC requirement	Owns decision and applicability	Understands service impact	Assists readiness interpretation	Provides service facts	Does not own contractor decision
FCI/CUI discovery	Owns business information	Traces technical paths	Facilitates/validates discovery	Identifies provider handling	Examines scope/evidence
Scope	Owns assessment boundary	Identifies MSP assets/services	Assists scoping analysis	Provides service architecture	Assesses defined scope
Architecture	Approves	Designs/implements assigned portions	Checks requirement alignment	Implements specialized portions	Evaluates implementation
SSP	Owns	Supplies technical facts	Assists accurate documentation	Supplies service descriptions/CRM	Examines
Daily operation	Accountable governance	Performs contracted operations	Usually not operator	Performs assigned service	Not operator
Evidence	Owns complete evidence story	Provides assigned evidence	Maps/tests readiness	Provides assigned evidence	Examines/tests/ interviews
Remediation	Authorizes/prioritizes	Implements assigned fixes	Tracks/readiness validates	Fixes assigned service	Evaluates according to assessment rules
Affirmation	Affirming official responsibility	Provides factual operational input	Supports factual readiness	Provides service evidence	Does not affirm for contractor
Continuous readiness	Owns program	Maintains assigned services	May support periodic review	Maintains assigned services	Independent reassessment when required

A.43 Checklist: Existing DoD Contractor Multi-Party Review

Question	Status	Owner	Evidence / Source	Action
Have all current DoD contracts and relevant flowdowns been reviewed?				
Can the contractor identify all FCI/CUI workflows already in operation?				
Has the MSP demonstrated every major administrative and security platform it uses for the customer?				
Have ESP relationships been evaluated using current CMMC scoping guidance?				

Do SSP, diagrams, responsibility matrix, service agreements, and live operation agree?				
Have subcontractors/suppliers receiving FCI/CUI been identified and applicable flowdown/status checks addressed?				
Can readiness personnel identify gaps without becoming the permanent operational owner?				
If C3PAO assessment is required, are assessment and implementation roles kept distinct?				
Can the contractor retrieve evidence without depending on one consultant or technician?				

A.44 Checklist: Prospective DoD Contractor Seeking Level 2

Question	Status	Owner	Evidence / Source	Action
Has the exact solicitation requirement been identified as Level 2 (Self) or Level 2 (C3PAO), rather than generically 'Level 2 certification'?				
Has the future FCI/CUI workflow been designed before protected contract information is accepted?				
Has a defensible assessment boundary been designed using current scoping guidance?				
Have MSP/ESP and specialized provider dependencies been selected and documented?				
Has the environment been technically implemented and operationally accepted?				
Do policies, procedures, SSP, diagrams, and responsibility matrix describe the implemented environment?				

Has representative operating evidence been generated truthfully?				
Have MSP technicians and contractor personnel demonstrated their actual workflows?				
Has the required assessment path been completed or scheduled according to the applicable award requirement?				
Are SPRS status, CMMC UID, and affirmation obligations understood for the solicitation?				
Is there an operational owner for the environment after implementation and assessment?				

A.45 The Multi-Party Handoff Test

A useful readiness test is to choose one event and follow it through all parties. Consider a new engineer joining a protected project. The contractor authorizes the employee and project access. The MSP creates or configures the identity and endpoint. A cloud provider supplies the underlying service. The SOC receives relevant security telemetry. The readiness documentation explains the process. Evidence records the authorization and technical result. During an applicable assessment, the assessor can examine, interview, or test the process.

Now reverse the event. The engineer leaves. The contractor triggers offboarding. The MSP removes access and recovers or secures the device. Specialized application access is removed. Remote sessions and privileged roles are checked. Evidence records the action. The SSP and responsibility model remain accurate.

If any party says, 'I thought the other company did that,' the handoff is not ready.

A.46 Final Multi-Party Readiness Standard

The contractor is ready when it can explain the requirement, the information, the boundary, the providers, the implementation, the evidence, and the continuing responsibilities. The MSP is ready when it can explain and demonstrate the exact services it performs, protect its privileged relationship with the customer, and produce evidence for its assigned functions. The readiness specialist is effective when the contractor and MSP can operate the program without depending on the specialist

to answer ordinary operational questions. The independent assessor, where required, can then evaluate a system whose story is already understood by the people who own and operate it.

The most important result of the multi-party model is not another diagram. It is the elimination of responsibility gaps. CMMC readiness depends on the connections between organizations just as much as it depends on the controls inside any one organization.

A.47 The Beginning-to-End Readiness Journey

A reader should be able to use this appendix even when the organization has never run a CMMC project. The starting point is not the firewall, Microsoft tenant, or a consultant's spreadsheet. The starting point is the business opportunity or existing contract and the information that will be handled while performing that work.

The practical sequence is: review the solicitation or contract; determine the required CMMC status and applicable information; map FCI and CUI workflows; define the assessment boundary; classify and inventory assets; identify MSP and other ESP dependencies; assign responsibilities; evaluate implementation against applicable requirements; design remediation and target architecture; implement; document; test; collect evidence; validate readiness; complete the applicable assessment path; maintain required status and affirmation; and operate continuously.

Each step produces information needed by the next step. If scope is guessed before information flows are understood, the inventory may be wrong. If technology is purchased before responsibility is assigned, two providers may each assume the other operates it. If evidence is considered only at assessment time, the organization may discover that a control worked but left no useful historical record.

A.48 Translating a Solicitation or Contract Into a CMMC Project

The contracting team identifies the actual clause, provision, level, system population, flowdown obligations, and timing that affect the opportunity. The readiness specialist can help organize the cybersecurity implications, but the MSP should not present itself as legal counsel merely because it understands CMMC technology.

The project team converts the contract review into technical questions: what information will be received; which users will perform the work; which locations will participate; which applications are required; whether subcontractors will receive information; what external exchange is necessary; and what system must have the required current CMMC status.

The output is a short requirements-and-assumptions record that becomes the foundation for scope. Assumptions that remain unresolved are tracked explicitly so that architecture is not built on an unspoken guess.

A.49 When CUI Markings or Handling Expectations Are Unclear

Real organizations sometimes receive information whose markings, dissemination controls, or handling expectations are unclear. The safe operational response is not

for a technician to make an improvised legal classification decision. The employee escalates through the contractor's designated contract, security, and CUI governance process.

The contractor preserves the source and context of the information, identifies the contract or program relationship, and seeks authoritative clarification through the appropriate channel. The MSP can restrict access or place the information in an approved protected workflow while the business question is resolved, but the MSP does not independently redefine Government information.

The readiness checklist should therefore ask whether employees know where uncertainty goes. A mature program has an escalation path for ambiguity instead of relying on individual memory.

A.50 Practical Level 2 Scoping and Asset Classification

Current DoD Level 2 scoping guidance treats the assessment boundary as more than the computers that visibly display CUI. The organization must understand CUI Assets and assets that provide security protections, as well as the treatment of specialized and other asset categories under the current guidance. External services can also matter when CUI or Security Protection Data resides on provider assets.

The working method is to start with each CUI workflow and follow it through identity, endpoints, applications, storage, networks, security systems, administration, backup, monitoring, and external providers. For every asset, the team records what it does, what data it handles, what protection it provides, who owns it, and why it has been categorized the way it has.

A classification label without rationale is weak. The useful evidence is the relationship between the asset, the information flow, the security function, and the current scoping rule. Significant architectural or boundary changes should trigger re-evaluation; current DoD guidance notes that significant changes such as network expansion or mergers and acquisitions can require a new assessment, while ordinary changes within an existing boundary that follow the SSP may be addressed through continuing compliance and affirmation.

A.51 Assessment Thinking: Examine, Interview, and Test

Readiness improves when the organization asks how an implementation would be demonstrated rather than merely whether a policy sentence exists. The CMMC Level 2 assessment materials use assessment methods that include examining artifacts,

interviewing personnel, and testing mechanisms. A mature readiness review therefore prepares for all three kinds of factual demonstration.

For an access-control activity, an examiner may review policy, configuration, authorization records, or logs. An interview may ask the system owner, administrator, or user to explain the process. A test may demonstrate the mechanism's behavior. The organization should not manufacture three separate stories; the same implementation should be visible through documentation, people, and technology.

Where these sources disagree, the discrepancy is itself a readiness finding. The objective is to correct the environment and documentation, not coach employees to repeat the document.

A.52 Building a Requirement-to-Evidence Trace

For each applicable requirement, the readiness team records the implementation statement, responsible party, systems involved, procedures used, evidence sources, and expected demonstration. This trace is not intended to replace the official assessment guide. It is an operational bridge between the requirement and the organization's real environment.

If NorthBridge operates vulnerability scanning, the trace should identify the scanner, coverage reconciliation, triage workflow, remediation tickets, exception process, verification, reporting, and the people who can demonstrate each portion. If Meridian owns approval of exceptions, that responsibility appears separately.

This approach prevents a common failure in which an organization owns many screenshots but cannot explain which implementation claim they support.

A.53 Physical CUI, Printing, Multifunction Devices, and Destruction

CUI may leave a digital system and become paper. The readiness review therefore follows printing from authorization through printer selection, physical possession, temporary storage, transport, and destruction. Multifunction devices are reviewed for storage, scanning, network connectivity, administration, and disposal implications according to their use.

The MSP may configure and secure the printer, while the contractor controls the physical workflow. Facilities, program management, employees, and records functions may own portions that IT cannot perform.

The test is practical: if an engineer prints a protected drawing today, can the organization explain where it may be printed, who can retrieve it, where it can be left, how it is transported, and how it is destroyed?

A.54 Removable Media, Mobile Devices, and Portable Storage

The organization determines whether removable media and mobile devices are prohibited, restricted, or approved for particular workflows. A blanket policy that says 'no USB' is not enough if manufacturing equipment requires approved removable media for legitimate work.

Where media is allowed, authorization, identification, protection, scanning, handling, storage, and sanitization or destruction are defined. Where it is prohibited, the organization checks whether technical and procedural enforcement align.

Mobile-device use is evaluated by information handled, management capability, authentication, encryption, applications, backup/synchronization behavior, remote wipe where applicable, and lost-device response.

A.55 Remote Work and Home Environments

Remote work is reviewed as an end-to-end information flow. The team identifies the managed endpoint, authentication path, approved collaboration and storage, remote support, printing, removable media, local caching, home-network assumptions, and incident reporting.

The goal is not to certify an employee's home network as though it were a corporate data center. The goal is to understand which protections the organization relies upon and to prevent unapproved paths that appear when the approved workflow is unusable.

A representative remote-work test should include ordinary work, a support interaction, an access denial where appropriate, and the response to a lost or compromised device.

A.56 Personnel Screening, Transfers, and Access Changes

Readiness includes the human lifecycle before, during, and after employment. The organization documents whatever screening and authorization processes apply to its roles and information, then connects those business decisions to technical provisioning.

A transfer is treated as an access event, not merely an HR record change. Project access that was appropriate yesterday may be excessive after reassignment. The same applies to contractors, temporary personnel, and vendor accounts.

Periodic access review should therefore compare technical entitlements with current business need rather than merely confirming that the user is still employed.

A.57 Media Sanitization, Device Disposal, and Reuse

When equipment leaves service, the organization determines what information may remain and what approved sanitization or destruction process applies. The process covers endpoints, servers, removable media, printer storage where relevant, backup media, and devices returned to vendors.

Asset disposition records should connect the asset identity to the action performed. Reuse inside the organization is also a data-handling event when a device moves from a protected role to another purpose.

The MSP may perform sanitization or coordinate disposal, but the contractor should know the process and retain appropriate evidence.

A.58 Secure Maintenance and Vendor Support

Maintenance can create temporary privileged paths into sensitive systems. The readiness review identifies who can perform maintenance, how access is authorized, what remote-support tools are allowed, how temporary credentials are controlled, and how sessions or actions are logged where appropriate.

A vendor that normally has no access may become highly privileged during troubleshooting. The temporary nature of the access does not make it irrelevant.

After maintenance, the team verifies that temporary access, accounts, firewall rules, or diagnostic files are removed or handled according to the approved process.

A.59 Time, Cryptography, Wireless, and Supporting Infrastructure

Some security mechanisms depend on infrastructure that users rarely notice. Accurate time supports log correlation and investigations. Cryptographic protection depends on approved implementation and key or certificate lifecycle. Wireless introduces authentication, segmentation, device, and coverage considerations. DNS and other foundational services can affect both security and availability.

The checklist therefore asks not only whether the primary business application is secure but whether the supporting services required by the protection architecture are deliberately managed.

These subjects should be tied to the applicable CMMC and NIST requirements during the detailed requirement mapping rather than treated as generic best-practice additions.

A.60 Configuration Baselines and Change Control

A secure environment needs a known starting condition. The organization defines approved configurations for important system classes and establishes how deviations are requested, approved, tested, implemented, and recorded.

Normal change control should be usable enough that technicians do not bypass it. Emergency changes require speed, but they still need authorization, validation, retrospective documentation, and any necessary update to the SSP, diagram, procedure, or evidence.

The readiness review samples real changes and follows them from request through verification. A policy saying changes are controlled is not equivalent to a demonstrable change process.

A.61 What Happens When Something Goes Wrong

CMMC readiness should be tested during failure. A missing EDR agent, silent firewall log source, failed backup restore, excessive technician privilege, stale application account, overdue vulnerability, unapproved file-sharing event, or broken security integration is not automatically proof that the entire program is meaningless. The key question is whether the operating model recognizes and manages the condition.

The response sequence is: detect or receive the issue; determine affected information and systems; assign ownership; assess urgency and contractual/security implications; contain or stabilize when needed; correct; retest; preserve evidence; update documentation or responsibility records if necessary; and identify what should prevent or detect recurrence.

If the organization discovers failures only during assessment preparation, its continuous-readiness mechanisms need improvement.

A.62 Failure Walkthrough: Missing EDR Agent

Inventory reconciliation shows a managed laptop in RMM but not in EDR. The MSP verifies that the device still exists and determines whether the agent was never installed, failed, was removed, or stopped communicating. The contractor determines whether the device participates in the protected environment and whether exposure requires additional response.

The MSP restores protection and validates communication. The team reviews the period of missing coverage, available telemetry, user activity, and any required investigation. The ticket preserves the cause, correction, and verification.

The systemic question follows: why did the coverage-reconciliation process not detect the condition sooner? Correcting the agent without correcting detection leaves the same weakness available to recur.

A.63 Failure Walkthrough: Firewall Logs Stop Reaching the SOC

The firewall may be functioning while the monitoring architecture is not. The SOC identifies source silence through source-health monitoring or the absence is discovered during review. The MSP checks connectivity, configuration, credentials/certificates, parser or collector health, and recent changes.

After restoration, HarborWatch-like monitoring personnel verify receipt and useful parsing, not merely packet transmission. The team determines whether the missing interval affects investigation capability and whether additional review is needed.

The evidence includes the alert or discovery, troubleshooting, correction, restored telemetry, and any process change designed to detect future silence.

A.64 Failure Walkthrough: Backup Is Green but Restore Fails

A successful backup job is not the same as successful recovery. When a representative restore fails, the team identifies whether the problem is corrupted data, missing credentials, application dependencies, incompatible configuration, insufficient documentation, or operator error.

The restore procedure is corrected and the test is repeated until the defined recovery outcome succeeds. Business owners verify that the recovered service is usable, not simply that files appeared.

The failed test is valuable evidence of governance when it shows detection, correction, retest, and improvement rather than being deleted from the record.

A.65 Failure Walkthrough: Departed User Retains Application Access

HR triggers offboarding and the central identity is disabled, but a specialized engineering application uses a separate local account. A negative-access test or later review discovers that the application identity remained active.

The organization removes the account, evaluates whether it was used after departure, and updates the offboarding inventory and procedure so specialized identities are included. Application ownership is clarified.

The lesson is that identity governance follows actual access paths, not just the directory service the MSP prefers to administer.

A.66 Failure Walkthrough: CUI Is Placed in an Unapproved Service

An employee uses a convenient consumer or public service to move a large protected file. The organization stops the unsafe workflow, preserves facts needed for investigation, follows its incident and contractual evaluation processes, and determines what information was exposed and what provider was involved.

The response should also ask why the employee chose the workaround. If the approved transfer method could not handle the file size or external recipient, training alone will not solve the underlying business problem.

The durable correction may require a better approved exchange method, technical restrictions, clearer procedure, and targeted training.

A.67 Failure Walkthrough: The MSP Changes Its RMM Platform

An MSP platform replacement is not merely an internal MSP purchasing decision when the platform provides administration, monitoring, scripting, patching, or evidence for a CMMC customer. The change may alter privileged paths, service identities, logs, retention, integrations, technician roles, and documentation.

Before migration, the contractor and MSP evaluate security and scope impact, update responsibility records, define parallel-operation or cutover testing, preserve required historical evidence, and validate customer separation and access.

After migration, old agents, accounts, API keys, firewall rules, and integrations are removed or closed deliberately. The SSP and diagrams are updated if the material architecture changed.

A.68 Major Organizational and Architectural Change Triggers

The readiness program defines events that require more than ordinary IT change review. Examples include acquisition or merger, a new facility, major network expansion, a new enclave, movement of CUI into a new cloud service, replacement of the MSP, significant provider change, a new line of DoD work, or a material change to the assessment boundary.

Current DoD Level 2 scoping guidance specifically notes that significant architectural or boundary changes can require a new assessment. The organization should therefore evaluate these events early rather than discovering after implementation that its prior assessment scope no longer represents the environment.

The program owner records the decision and supporting rationale, including whether reassessment, documentation updates, provider review, or additional contractual coordination is needed.

A.69 New SaaS, AI, and Integration Readiness Gate

New SaaS and AI services are evaluated before protected information is placed into them. The requesting business owner describes the intended data and workflow. Security and contract personnel evaluate applicable handling requirements. The MSP evaluates identity, administration, endpoints, logging, integrations, and technical enforcement.

An API integration receives the same attention because automated data movement can create a new information flow even when employees never open the destination application manually.

The readiness gate records whether the service is approved for protected information, approved only for ordinary business data, requires conditions, or is not approved. This prevents procurement from silently changing the CMMC boundary.

A.70 Provider Exit and MSP Transition Readiness

The organization should know how it will leave a provider before the relationship ends. Exit planning identifies customer data, configuration, logs, documentation, credentials, domains, licenses, backups, administrative roles, integrations, and evidence that must be transferred, retained, or destroyed.

When replacing an MSP, the outgoing provider should not remain the only party that understands the environment. The incoming provider needs controlled knowledge

transfer and validated access while old privileged access is removed at the appropriate time.

The contractor verifies closure rather than assuming cancellation of an invoice removed technical access.

A.71 Readiness Prioritization When Everything Cannot Be Fixed at Once

Organizations often discover more work than they can complete simultaneously. Prioritization considers contractual deadlines, requirement eligibility, exposure of CUI, privileged-access risk, known exploitation, scope impact, dependencies, operational feasibility, and the time needed to generate reliable evidence after implementation.

The team distinguishes prioritization from permission to defer. An issue being lower on the project list does not mean an applicable requirement can legally or contractually remain unmet. POA&M eligibility is governed by the applicable CMMC rules and must be verified.

Management receives the unresolved-condition list with consequences and dependencies so resource decisions are informed rather than hidden inside technical tickets.

A.72 Executive Readiness Gate

Before the organization proceeds to the applicable assessment or relies on a CMMC status for an award, senior management should receive an evidence-based readiness briefing. The briefing is not a consultant's confidence score. It identifies what has been verified, what remains unresolved, what assumptions remain, what providers are critical, what material changes are underway, and what management is being asked to affirm or represent.

The affirming official should have a factual basis for the required annual affirmation. Current DFARS 252.204-7021 requires annual affirmation of continuous compliance in SPRS for each applicable CMMC UID and requires current status for the systems used to process, store, or transmit the relevant FCI or CUI.

Management should stop the readiness gate when a material fact is unknown rather than converting uncertainty into optimism.

A.73 Executive Readiness Gate — Working Table

Executive Question	Verified?	Evidence / Owner	Unresolved Condition / Decision
Do we know the exact CMMC status required for the opportunity or contract?			
Can we identify and explain every material FCI/CUI flow?			
Does the assessment boundary match the live environment?			
Can we explain the role and scope impact of every critical MSP/ESP/provider?			
Do responsibility documents match contracts, procedures, and actual operation?			
Can ordinary operators demonstrate the controls they perform?			
Can we retrieve current and historical evidence without depending on one consultant?			
Have significant failures been corrected, retested, and evaluated for recurrence?			
Are unresolved deficiencies and POA&M eligibility accurately understood?			
Have significant architectural/boundary changes been evaluated for reassessment impact?			
Is the affirming official receiving a complete factual picture?			
Can the environment continue operating securely the day after the assessment?			

A.74 Final Appendix A Readiness Standard

Appendix A is complete only when it leads the organization from business requirement to sustained operation. The contractor should be able to identify the requirement and information, defend the scope, explain the provider ecosystem, assign responsibilities, demonstrate implementation, retrieve evidence, manage failures, support the applicable assessment, and continue operating after the assessment. The MSP should be able to demonstrate its assigned technical functions without claiming ownership of the contractor's entire compliance obligation.

Readiness specialists should strengthen the organization's capability rather than become permanent substitutes for it.

The final test is operational. If a new contract arrives, an employee leaves, a security agent disappears, a cloud service changes, a provider is replaced, or an assessor asks an unexpected question, the organization should know how to determine what matters next. That capability—knowing the environment, assigning the right owner, acting, verifying, preserving evidence, and updating the system story—is the foundation on which the remaining appendices build.

Appendix B

MSP Scoping Checklist

A Detailed Contractor–MSP–ESP Scoping and Boundary Workbook

Dr. Charles Edwards

B.1 Purpose of This Appendix

This appendix answers one of the most difficult practical questions in CMMC operations: when does an MSP, MSSP, cloud service, security platform, technician, or other external provider become relevant to the contractor's CMMC assessment scope? The answer cannot be reduced to a vendor name or a contract label. Scoping follows the functions actually performed, the information actually handled, the security capabilities actually provided, and the administrative paths that actually exist.

Appendix A established the multi-party model. Appendix B applies that model specifically to scope. The contractor or offeror remains the center of the analysis because it is the organization seeking assessment or performing the covered work. The MSP and other External Service Providers must then be examined service by service. The readiness specialist helps the parties map those facts to current CMMC scoping guidance. A C3PAO, when an independent Level 2 assessment is applicable, evaluates the defined assessment scope rather than designing the contractor's architecture.

B.2 Current Regulatory Context and Why Scoping Must Be Date-Aware

As of September 2026, DoD has suspended CMMC Phase II implementation while Phase I self-assessment requirements remain in place. That implementation posture does not eliminate the underlying requirement to protect CUI under applicable DFARS obligations, and organizations should continue to use the current official CMMC scoping and assessment resources while monitoring for reform changes.

The current DoD Level 2 Scoping Guide identifies CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets and provides additional treatment for External Service Providers. Because CMMC is currently under review, this appendix teaches a durable scoping method while directing the reader to verify the current official guidance before making a final assessment-boundary decision.

B.3 Scoping in Plain English

Scoping is the process of deciding which people, technologies, facilities, services, and information flows matter to the assessment and why. It is not simply drawing a box around the company's office or listing every device owned by the business.

A useful starting question is: where can CUI go, what can act on it, and what protects the environment in which it exists? The team follows CUI from receipt or creation through use, storage, transmission, collaboration, backup, printing, monitoring, administration, archival, and destruction. It then follows the security systems that protect those paths.

The scoping story must be understandable by both management and technicians. Management should understand why a service is relevant; technicians should be able to show how it connects.

B.4 The MSP Is Not Automatically In Scope—and Is Not Automatically Out of Scope

A contractor should not assume that hiring an MSP automatically places the MSP's entire corporate environment inside the customer's assessment scope. The opposite assumption is equally dangerous. Calling a provider 'external' does not make its service irrelevant.

The current Level 2 Scoping Guide states that an ESP that processes, stores, or transmits CUI is a CUI Asset and must meet the applicable requirements. It also explains that an ESP providing a security protection function can be a Security Protection Asset even when it does not process CUI. The practical analysis therefore examines the actual service, provider assets involved, data handled, and security capability delivered.

The unit of analysis should be the service and its technical relationship to the assessed environment, not merely the legal entity name.

B.5 CUI Assets

A CUI Asset processes, stores, or transmits CUI. Processing includes using, accessing, editing, generating, manipulating, or printing the information. Storage includes electronic and physical forms. Transmission includes digital and physical transfer.

For an MSP, obvious examples may include a provider-hosted file service that stores customer CUI or a support workflow that receives CUI files. Less obvious examples arise when a technician downloads a protected file for troubleshooting or when a ticket attachment contains the customer's CUI.

The MSP should therefore test its assumptions against real workflows. 'Our contract says we do not store CUI' is not evidence that no technician has ever attached a CUI file to the PSA.

B.6 Security Protection Assets and Security Protection Data

Security Protection Assets provide security functions or capabilities within the contractor's assessment scope. Current DoD guidance uses a SIEM service as a direct example: the SIEM may be logically separated and may not process CUI, yet it contributes to meeting CMMC requirements and is therefore relevant as a Security Protection Asset.

Security Protection Data is security-relevant information used to protect the assessed environment. Examples can include security configuration information, log data, vulnerability information, and other information whose disclosure could assist an attacker. The MSP must understand that 'not CUI' does not automatically mean 'not relevant to scope.'

This is why an MSP's EDR console, vulnerability platform, SIEM, RMM, identity administration, and other security systems require careful analysis even when customer CUI is intentionally excluded from them.

B.7 Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets

The current scoping framework also recognizes asset categories whose treatment differs from ordinary CUI Assets. The organization should apply the definitions and requirements in the current official guide rather than inventing local labels.

Contractor Risk Managed Assets require deliberate documentation and risk-based treatment under the current guidance. Specialized Assets can include systems such as operational technology, IoT, test equipment, restricted information systems, and government-furnished equipment where the current guide's definition applies. Out-of-Scope Assets must satisfy the current exclusion logic rather than simply being declared unimportant.

The MSP should document why an asset received its category and what technical facts support the decision. An unexplained spreadsheet label is not a defensible boundary.

B.8 Start With the Information Flow, Not the Tool List

Many MSP scoping exercises fail because they begin with a list of products: Microsoft 365, firewall, RMM, EDR, backup, PSA, SIEM. The team then debates whether each product is 'in scope.' A better method begins with the contractor's work.

Choose a representative CUI item and follow it. How is it received? Which identity opens it? Which endpoint displays it? Where is it saved? How is it shared internally? How does it reach a subcontractor? Is it printed? Is it backed up? Which security tools monitor the endpoint? Which administrator can change the controls? Which logs prove what happened?

The product list becomes meaningful only after it is connected to those flows.

B.9 The Three Administrative Paths Every MSP Should Map

The first path is the user path: how ordinary contractor personnel access and use protected systems. The second is the privileged path: how MSP technicians, internal administrators, vendors, and automated service identities administer those systems. The third is the security-telemetry path: where logs, alerts, vulnerability information, endpoint events, backup status, and other protection data travel.

These paths frequently cross organizational boundaries. A user may remain entirely inside the contractor tenant while a privileged MSP technician connects from an MSP-managed workstation through an RMM platform. Security telemetry may then leave the contractor environment for a separate SOC platform.

Each path must be mapped independently because a design that controls the user path but ignores the administrator or telemetry path is incomplete.

B.10 RMM Platforms

Remote Monitoring and Management platforms are among the most important MSP scoping subjects because they can provide broad administrative power. An RMM agent may execute commands, deploy software, transfer files, run scripts, manage services, collect inventory, initiate remote sessions, and sometimes expose credentials or integrations.

The scoping review records the RMM vendor and service, tenant separation, customer instances, agent coverage, technician identities, MFA, privileged roles, script libraries, file-transfer capability, audit logging, API integrations, retention, administrative workstations, and subcontracted support.

The team must also determine whether CUI can enter the RMM workflow. A remote session that merely displays a user's desktop may create different handling facts than an RMM file-transfer function that copies a protected drawing into provider-controlled storage.

Operational evidence should show who can administer the customer, how access is approved, how terminated technicians are removed, how agents are reconciled, and how anomalous or unauthorized administrative actions are detected.

B.11 PSA and Ticketing Systems

A Professional Services Automation or ticketing platform may appear to be a business-management system, but support tickets can accumulate technical details, screenshots, configuration data, credentials, logs, and user attachments. The scoping question is therefore based on actual ticket content and workflow.

The MSP should establish explicit rules about CUI in tickets. If CUI is prohibited, technicians need a safe alternative for receiving or viewing protected information during support. The MSP should also evaluate whether security protection data in tickets makes portions of the service relevant even when CUI is prohibited.

Ticket templates should encourage references and secure links rather than unnecessary copying of protected content. Training must explain what to do when a customer attaches CUI despite the policy.

B.12 Credential Vaults and Privileged Access Management

A credential vault may contain passwords, API secrets, recovery codes, privileged-account metadata, and other information capable of opening the contractor's protected environment. The fact that the vault does not store CUI does not make its compromise harmless.

The review covers vault architecture, encryption, MFA, role design, technician access, emergency access, shared versus named credentials, checkout or retrieval logs, rotation, offboarding, API integrations, backup, recovery, and administrative ownership.

Where possible, the operational model should reduce standing privilege and make technician actions attributable to individuals. Shared administrative credentials without compensating accountability create both security and evidence problems.

B.13 MSP Technician Workstations

The technician's endpoint can become part of the practical security boundary because it is the launching point for privileged administration. The scoping team asks whether technicians administer customer systems through managed devices, what endpoint controls apply, whether local storage is possible, whether clipboard or file transfer can move customer data, and whether browser profiles or cached credentials persist.

A provider cannot reason only about the customer's endpoint while ignoring the computer from which powerful administrative commands originate. The exact scoping treatment depends on the service architecture and current guidance, but the risk and administrative path must be understood.

The MSP should be able to demonstrate its technician onboarding, device compliance, MFA, privileged-role assignment, logging, and offboarding processes for personnel who administer the customer.

B.14 Microsoft 365, GCC, GCC High, and Tenant Administration

Microsoft Government cloud decisions require separate analysis of the contractor tenant and the provider's administrative relationship. GCC and GCC High are cloud environments, not software packages installed on a workstation. The contractor's eligibility, contractual and regulatory requirements, information types, service capabilities, and provider commitments should drive the environment decision.

The MSP scoping review maps tenant administrators, delegated administration, emergency accounts, Conditional Access, MFA, Exchange, SharePoint, OneDrive, Teams, Intune, Defender, Purview where used, service identities, applications, APIs, domains, DNS, licensing, logging, and external sharing.

An implementation provider may build the tenant and leave after migration while the MSP becomes the steady-state administrator. The scope and responsibility documentation must show that handoff explicitly. Buying GCC High alone does not establish CMMC compliance; the tenant still has to be configured, operated, documented, evidenced, and integrated into the contractor's overall system.

B.15 EDR and Endpoint Security Platforms

An EDR platform provides a security protection capability and commonly receives detailed endpoint telemetry. The scoping analysis identifies which assets are covered, what telemetry is collected, where it is stored, who can query it, who can isolate devices, how exclusions are controlled, and how alerts are handled.

Coverage reconciliation is essential. The contractor and MSP should compare authoritative asset inventory, RMM, EDR, device management, and other relevant sources to identify endpoints that silently disappeared from protection.

Evidence should demonstrate not only that the product is licensed but that agents are healthy, policies are applied, alerts are reviewed, exclusions are governed, and failures are corrected.

B.16 Vulnerability Management Platforms

Vulnerability platforms may contain Security Protection Data such as asset identities, software versions, missing patches, vulnerabilities, exposure details, and remediation status. The review maps scanner placement, agents, credentials, scan coverage, cloud consoles, integrations, technician roles, retention, ticket creation, exceptions, and verification.

The MSP must distinguish scanning from remediation. A provider may operate the scanner while the contractor owns application-risk decisions, or the MSP may patch operating systems while a specialized vendor patches an engineering application.

The responsibility matrix must identify these seams so an open vulnerability does not remain unresolved because every party believes another party owns it.

B.17 Backup and Recovery Providers

Backup requires a direct data-content analysis. If protected files, mailboxes, virtual machines, databases, or endpoints containing CUI are backed up, the backup service may store CUI. The team maps data location, encryption, administration, retention, immutability where used, recovery access, support access, deletion, and provider/subprocessor relationships.

The MSP also maps who can initiate restore, where restored data can be placed, how recovery is tested, and what evidence demonstrates successful recovery. A backup dashboard showing green jobs is not sufficient evidence that the organization can recover its protected operation.

Provider exit planning must address retained backup copies and the lifecycle of customer data after termination.

B.18 SIEM, SOC, and MSSP Services

A SIEM or SOC service may never receive the customer's business documents but can still be central to the CMMC environment because it provides security protection.

Current DoD scoping guidance explicitly uses a SIEM ESP as an example of a Security Protection Asset.

The review maps log sources, collectors, agents, transport, normalization, storage, retention, correlation, alerting, analyst access, escalation, case management, evidence retrieval, and source-health monitoring.

The contractor should know what happens when an expected log source goes silent. The SOC should know whom to contact. The MSP should know who repairs the collection path. The responsibility matrix should identify all three.

B.19 Firewalls, Networks, VPN, and Remote Access

Network security scope follows the CUI and administrative paths. Firewalls, VPN gateways, segmentation devices, wireless infrastructure, DNS services, and remote-access technologies may provide security protection to the assessed environment.

The MSP documents configuration ownership, privileged access, rule approval, remote-access methods, MFA, logging, firmware management, backup configuration, change control, and monitoring.

Temporary vendor access deserves particular attention. A connection used only during equipment maintenance can still create a privileged path into the environment.

B.20 Cloud, SaaS, and File-Exchange Services

Every cloud or SaaS service is evaluated according to what information it handles and what security function it performs. The question is not whether the vendor is well known. The question is how the service participates in the contractor's protected workflow.

File-exchange services are especially important because employees often adopt them to solve size or external-sharing problems. The approved architecture should provide a usable method for legitimate external exchange so that employees are not pushed toward consumer services.

API integrations are treated as data flows. Automated transfer does not make information disappear from scope.

B.21 Printers, Scanners, MFDs, and Physical Workflows

An MSP may manage printers while the contractor manages physical CUI. The scoping exercise evaluates whether devices process or store protected information,

whether scans are transmitted, whether internal storage exists, who administers the device, and how it is sanitized at disposal.

The physical side of the workflow includes printed output, secure pickup, storage, transport, reproduction, and destruction. The MSP may own device configuration without owning every physical handling procedure.

B.22 OT, Manufacturing, Test Equipment, and Specialized Assets

Defense manufacturers often have systems that cannot be managed like ordinary office endpoints. CNC support systems, test stations, laboratory equipment, embedded devices, industrial controllers, engineering workstations, and government-furnished systems can introduce specialized scoping questions.

The current Level 2 Scoping Guide contains a Specialized Asset category. The contractor should document how the current definition applies, the asset's role in the CUI workflow, applicable protections, network relationships, maintenance, vendor access, and risk treatment.

The MSP should avoid forcing an ordinary workstation control pattern onto equipment where it is technically unsafe or unsupported; the architecture should instead document the real constraints and appropriate protection strategy.

B.23 MSP Subcontractors and the Provider Chain

An MSP may rely on a SOC provider, help-desk subcontractor, cloud distributor, backup vendor, vulnerability platform, documentation system, remote-support platform, or after-hours service. The contractor's dependency therefore may extend beyond the company whose logo appears on the MSP agreement.

The MSP should maintain a provider-chain map for CMMC customers. For each upstream or subcontracted service, the map records function, data, privileged capability, responsibility, evidence, contractual commitments, and termination path.

A provider chain that cannot be explained is a scoping and continuity weakness.

B.24 CSP Versus Other ESP Treatment

The current Level 2 Scoping Guide distinguishes treatment of a cloud service provider used to process, store, or transmit CUI from other ESP scenarios and references the applicable FedRAMP Moderate equivalency requirement arising from DFARS 252.204-7012.

The contractor and MSP should therefore identify whether a service is functioning as a CSP for CUI, as another type of ESP, as a Security Protection Asset service, or in multiple roles. The label should follow the actual service rather than marketing terminology.

Current official guidance should be checked before the final architecture or assessment because cloud and ESP treatment is a high-consequence area.

B.25 Scoping the Readiness Specialist

A readiness consultant may have access to SSP drafts, network diagrams, inventories, evidence, vulnerability information, policies, and other sensitive security information. The consultant's role should be examined even if the consultant never administers the production environment.

The organization defines where documents are exchanged, what the consultant may retain, how access is authenticated, how evidence is protected, and what happens at engagement end.

The consultant should not become an uncontrolled shadow repository for the contractor's CUI or security protection information.

B.26 Scoping the C3PAO Assessment Interaction

The independent assessor receives access to evidence and demonstrations needed for the assessment. The organization should plan how assessment evidence will be presented without creating unnecessary new copies or unmanaged data flows.

The MSP identifies which technicians may be interviewed or asked to demonstrate assigned functions. The contractor remains responsible for coordinating the assessment and explaining its system.

The assessment interaction should not require last-minute creation of uncontrolled file-sharing channels.

B.27 The MSP Service-by-Service Scoping Interview

The most effective MSP scoping interview is conducted with people who actually operate the tools. For each service, the team asks what it does, where it is hosted, what customer information enters it, what security data enters it, what privileged actions it enables, which technicians can access it, what integrations exist, what evidence it produces, and which subcontractors support it.

The interviewer then asks failure questions. What happens if the service is unavailable? What happens if a technician leaves? What happens if an API key is compromised? What happens if a customer accidentally uploads CUI? What happens when the MSP changes vendors?

These questions expose real boundaries better than a product brochure.

B.28 MSP Scoping Worksheet

Service / Asset	CUI?	Security Protection Function/Data?	Privileged Path?	Provider / Subprovider	Proposed Category	Rationale / Evidence
RMM						
PSA / ticketing						
Credential vault / PAM						
Technician workstations						
Microsoft tenant administration						
EDR						
Vulnerability platform						
Backup / recovery						
SIEM / SOC						
Firewall / VPN management						
Documentation platform						
File exchange						
Cloud / SaaS integrations						
After-hours support						

B.29 Technician Access Worksheet

The technician-access worksheet should be completed for each class of personnel who can administer the customer. Named access is preferable for accountability

where technically feasible. The team records source device requirements, authentication, privilege, customer separation, approval, monitoring, and offboarding.

B.30 Technician Access Working Table

Technician Role	Source Device	Authentication/ MFA	Customer Privilege	Approval	Logs / Evidence	Offboarding Test
Help Desk						
Systems Administrator						
Network Engineer						
Cloud Administrator						
SOC Analyst						
Escalation Engineer						

B.31 Data-Flow Worksheet

For each representative CUI workflow, record the source, destination, identity, endpoint, application, network path, storage, backup, monitoring, external providers, and physical handling. Then repeat the exercise for the privileged-administration path and the security-telemetry path.

A complete scope diagram should be understandable without oral folklore. If a line crosses an organizational boundary, label the provider and service. If a system provides security protection, show that relationship even when CUI does not flow through it.

B.32 When a Ticket Accidentally Receives CUI

The MSP should have a predefined response rather than improvising. The technician stops unnecessary distribution, preserves enough information to understand what occurred, notifies the designated customer/MSP contacts, follows the applicable incident and handling process, moves the work to an approved channel, and addresses the unauthorized copy according to the approved retention and deletion procedure.

The event is then used to test the design. If customers repeatedly attach CUI to tickets, the support workflow may need technical controls, clearer instructions, or a secure upload mechanism.

B.33 When an MSP Technician Downloads CUI During Troubleshooting

A technician may believe a local download is the fastest way to diagnose a problem. That action can create a new CUI location and change the facts underlying scope. The service design should therefore specify whether local download is permitted, prohibited, or restricted to an approved controlled environment.

If the workflow requires access to content, the MSP and contractor should design a method that minimizes copies and keeps the technician inside an approved administrative path. Training must match the technical reality.

B.34 When a Backup Provider Stores CUI

If backup data includes CUI, the provider relationship is evaluated accordingly. The organization documents the service architecture, data location and protection, contractual commitments, recovery workflow, provider access, and the current requirements applicable to a cloud service used for CUI.

The MSP cannot treat backup as merely an availability product when the backup contains the same protected information as the production system.

B.35 When the SIEM Contains No CUI but Protects the Environment

This is the classic Security Protection Asset example. The SIEM's relevance arises from the security capability it provides and the Security Protection Data it handles. The assessment team needs to understand how the service supports applicable requirements, who operates it, and how evidence is obtained.

The scope story should therefore include both information-bearing systems and protection systems.

B.36 When the MSP Replaces a Tool

A tool replacement triggers a scope review when it changes data flow, privileged access, security function, provider relationship, or evidence. The MSP notifies the contractor before material migration, maps old and new capabilities, tests the new service, preserves required historical evidence, updates documentation, and removes obsolete access.

An MSP's internal standardization project can become a customer CMMC change even when the customer did not request it.

B.37 When the Contractor Changes MSPs

The contractor maps all access held by the outgoing MSP: named and shared accounts, delegated administration, RMM agents, VPN accounts, API keys, firewall access, vault records, backup consoles, cloud roles, documentation portals, and subcontracted services.

Knowledge and evidence are transferred deliberately. The incoming MSP validates the environment rather than assuming the predecessor's documentation is current. The outgoing provider's access is removed and tested.

The contractor should be able to continue the program without losing the historical evidence needed to explain prior operation.

B.38 Scoping Change Triggers

Scope should be re-evaluated when CUI workflows change, a new contract or program arrives, a facility is added, remote work changes, a new cloud or SaaS service is approved, an MSP tool changes, a provider is replaced, a merger or acquisition occurs, network boundaries expand, a new subcontractor receives CUI, or a specialized system is connected.

The review records what changed, which diagrams and inventories are affected, whether asset categories changed, whether the SSP or responsibility matrix must change, and whether the current assessment status remains representative under current rules.

B.39 Management Scoping Gate

Management should not approve the final boundary until the contractor and MSP can explain the same environment consistently. The boundary is not ready if one party believes a service is out of scope while the other relies on that service to meet a requirement.

The final management package should contain the information-flow diagrams, asset inventory and categories, provider/service map, responsibility matrix, major assumptions, unresolved questions, and the evidence supporting consequential provider decisions.

B.40 Final MSP Scoping Checklist

Final Scoping Question	Status	Owner	Evidence / Rationale	Action / Review Date

Have all representative CUI flows been mapped end to end?				
Have user, privileged-administration, and security-telemetry paths been mapped separately?				
Has every MSP service been analyzed by function rather than vendor label?				
Are CUI Assets identified and documented?				
Are Security Protection Assets and Security Protection Data relationships identified?				
Have Contractor Risk Managed, Specialized, and Out-of-Scope asset decisions been documented using current guidance?				
Has RMM file transfer, scripting, remote control, API, and technician access been evaluated?				
Has PSA/ticket content been reviewed for CUI and security protection data?				
Have credential vaults and privileged identities been mapped?				
Have technician workstations and source administrative devices been evaluated?				
Has Microsoft/cloud delegated administration been mapped?				
Have EDR, vulnerability, backup, SIEM/SOC, firewall, and VPN services been evaluated?				
Have cloud/SaaS/API integrations been mapped as data flows?				
Have MSP subcontractors and upstream providers been identified?				
Has CSP versus other ESP treatment been evaluated under current official guidance?				

Have physical, printing, MFD, remote-work, OT, and specialized workflows been considered?				
Does the SSP describe provider relationships and responsibilities accurately?				
Does the network/data-flow diagram show provider boundaries and security services?				
Can MSP technicians demonstrate assigned functions and produce evidence?				
Are provider exit and MSP transition procedures defined?				
Are scoping change triggers part of change management?				
Have current DoD scoping resources been rechecked before final assessment decisions?				

B.41 Final Teaching Standard

MSP scoping is complete when the contractor can explain not only where CUI resides but how the entire protected environment is operated and defended across organizational boundaries. The MSP should be able to identify every service it performs for the customer, every privileged path it uses, every relevant data type it receives, every upstream provider it depends upon, and every evidence source it is expected to produce.

The most useful final question is not 'Is our MSP in scope?' It is: 'Which MSP services, assets, people, data, and administrative relationships matter to this assessment, under which current scoping category or provider rule, and what evidence supports that conclusion?' That question forces the parties to reason from the actual architecture rather than from assumptions.

B.42 Building the Scope From the Contract Backward

The most defensible scope begins with the contract or solicitation and works backward into technology. The team identifies what information the organization will create, receive, use, and deliver in performance of the covered work. It then identifies the business processes and people that perform those activities before identifying the systems supporting them.

This sequence prevents a common mistake: allowing the MSP's standard technology stack to define the contractor's CMMC environment. The stack supports the environment; it does not define the business obligation. A contractor may use the same Microsoft tenant, RMM, firewall, and EDR as another customer while having a very different CUI workflow and assessment boundary.

For an existing contractor, this exercise should include actual contracts, task orders, delivery orders, subcontracts, program instructions, CUI markings, and current workflows. For a prospective offeror, the team records assumptions about the anticipated workflow and validates them as award and program information becomes available.

B.43 Business Process Scoping Before Technical Scoping

Before drawing a network diagram, identify the departments and business processes that touch the covered work. Engineering, estimating, contracts, quality, manufacturing, project management, finance, shipping, field service, and executive personnel may interact with different information at different points.

A person does not become relevant merely because of a job title. The team asks what work the person performs, what information the person receives, what applications are used, where work occurs, and whether protected information can be created or reproduced.

This business-process map is particularly useful when a company believes that CUI exists only in engineering. A purchase specification, quality record, production traveler, support ticket, or subcontractor package may carry the same protection obligation into another department.

B.44 Facility and Location Scoping

Scope must account for where protected work occurs. Headquarters, branch offices, manufacturing floors, laboratories, warehouses, temporary project locations,

employee homes, customer sites, and shared facilities can create different technical and physical protection requirements.

The MSP maps connectivity and managed technology, while the contractor maps physical access and business use. A small branch with one engineer may be more relevant than a large sales office if the engineer performs covered work there.

Location diagrams should identify network connections, wireless, printers, local servers, physical storage, visitor exposure, remote access, and provider-managed equipment where applicable.

B.45 Identity as a Scoping Backbone

Identity connects users, administrators, devices, cloud services, and evidence. The team identifies the authoritative identity sources, federation, synchronization, local accounts, cloud-only accounts, service accounts, emergency accounts, vendor identities, shared accounts, and machine identities used in the protected environment.

The MSP should map delegated administration separately from ordinary customer identities. A technician may never appear in the contractor's HR roster yet hold powerful administrative capability through a partner portal, RMM, VPN, or vendor platform.

Identity scoping also exposes hidden dependencies. If an out-of-scope corporate directory authenticates users into the CUI environment, the team must examine that relationship rather than relying on a diagram that simply places the directory outside a boundary.

B.46 Service Accounts, API Keys, Tokens, and Non-Human Identities

Modern environments depend on non-human identities. Backup agents, monitoring collectors, scanners, applications, scheduled tasks, service principals, API integrations, automation platforms, and security tools may authenticate without a person typing a password.

The scoping inventory records purpose, owner, privilege, authentication material, storage, rotation, logging, dependencies, and decommissioning. An API token capable of administering a protected tenant deserves the same seriousness as a privileged human account.

Provider changes frequently leave orphaned non-human identities. The MSP transition checklist should therefore include service principals, application registrations, API keys, certificates, automation accounts, and integration secrets.

B.47 Virtualization, Hypervisors, VDI, and Remote Desktop Infrastructure

Virtualization can concentrate many protected systems on a small number of highly privileged infrastructure components. Hypervisors, management consoles, storage fabrics, virtual networking, snapshots, templates, and backup integration should be evaluated according to the functions and data they support.

VDI and remote desktop can be powerful scope-reduction tools when designed carefully because users may interact with CUI without placing persistent copies on ordinary endpoints. That benefit depends on configuration. Clipboard, drive mapping, printing, file transfer, browser downloads, screenshots, and local synchronization can reopen paths that the architecture was intended to close.

The team validates the actual user experience rather than assuming the word 'VDI' creates a boundary.

B.48 Servers, Storage, NAS, SAN, and Shared File Systems

On-premises servers and storage are mapped by role, data, administration, network segment, backup, monitoring, patching, and physical location. Shared storage deserves special attention because permissions and inheritance can silently broaden access.

The MSP documents management interfaces and administrative paths, including out-of-band management where present. The contractor identifies which shares, databases, or applications support covered work.

Snapshots, replication targets, archives, and disaster-recovery copies are included in the data lifecycle. A secondary copy remains relevant even when users rarely access it.

B.49 Email as a CUI Path

Email frequently becomes a CUI transmission and storage path because customers, primes, subcontractors, and employees exchange documents through ordinary business communication. The team identifies approved mail systems, encryption or protected-message mechanisms where required, external recipients, forwarding, mobile access, journaling or archiving, backup, and administrative access.

Policies should not assume that employees can recognize every sensitive attachment perfectly. Technical and procedural safeguards should reinforce the approved workflow.

The MSP must also examine mail-security gateways and third-party filtering services because messages or attachments may transit or be retained by those providers.

B.50 Collaboration Platforms and External Sharing

SharePoint, Teams, OneDrive, and other collaboration platforms can centralize protected work, but external sharing, guest access, synchronization, unmanaged devices, link settings, application integrations, and retention can materially change the information flow.

The scoping team maps where sites and libraries are used for CUI, who owns them, who can invite guests, what synchronization is allowed, and how departed users or external collaborators are removed.

A secure collaboration platform becomes less secure when employees export content into unmanaged workflows to overcome usability limitations. Scoping interviews should therefore ask how people actually share large files and collaborate with subcontractors.

B.51 Source Code, Repositories, DevOps, and CI/CD

Software development organizations may place CUI or controlled technical information in source code, issue trackers, build artifacts, test data, documentation, repositories, pipelines, package registries, and deployment systems.

The team maps repository hosting, developer endpoints, secrets, branch protections, CI/CD runners, build agents, artifact storage, cloud integrations, administrative roles, and third-party development tools.

A development pipeline can move information automatically across several services. Each integration should be treated as an information and privilege path, not merely a developer convenience.

B.52 Engineering Applications and CAD/CAM Workflows

Engineering environments often contain some of the most consequential CUI while depending on specialized applications, license servers, file formats, plotters, manufacturing interfaces, and vendor support.

The scoping review follows drawings and models from receipt or creation through editing, collaboration, revision control, export, manufacturing, backup, and delivery. Temporary files, autosave folders, render caches, and local workspaces should not be ignored merely because they are not the official document repository.

Vendor remote support and licensing infrastructure are mapped separately because they may create administrative or network dependencies without receiving the engineering data itself.

B.53 Databases, ERP, CRM, and Business Applications

Protected information can enter business applications outside the traditional document repository. ERP records, quality systems, project systems, CRM notes, procurement records, and custom databases may contain contract-related technical or operational information.

The team examines fields, attachments, reports, exports, integrations, administrator access, backup, and support. It does not classify an entire application based on one screen without understanding the data model and actual use.

Where an application is intentionally kept outside the CUI environment, the organization should define what information may and may not be entered and provide an approved alternative workflow.

B.54 Logs Are a Data Flow Too

Security and operational logs can contain usernames, hostnames, IP addresses, paths, command lines, filenames, application events, configuration details, and other Security Protection Data. Some logs may also capture protected content depending on the application and configuration.

The team maps log generation, collection, forwarding, enrichment, storage, analyst access, retention, export, and deletion. It also identifies whether a support provider can search or download customer telemetry.

Logging architecture should minimize unnecessary sensitive content while retaining the information needed for security, investigation, and assessment evidence.

B.55 Monitoring the MSP's Own Privileged Environment

When an MSP administers a customer's protected environment, the MSP's own identity, endpoint, and security practices can materially affect the customer. The provider should therefore be able to explain how privileged technicians are authenticated, how their devices are managed, how access is logged, and how misuse or compromise would be detected.

This does not mean the customer's CMMC scope automatically becomes the MSP's entire enterprise. It means the service relationship must be analyzed accurately, and

the relevant provider assets and capabilities must be treated according to current scoping rules.

The MSP should resist both extremes: claiming that every corporate system is part of every customer assessment, or claiming that nothing at the MSP matters because the customer owns the CUI.

B.56 Shared MSP Platforms and Multi-Tenant Risk

MSPs achieve efficiency by sharing platforms across customers. RMM, PSA, documentation, EDR management, backup consoles, SIEM, identity portals, and automation may be multi-tenant. Scoping must therefore address tenant separation and the possibility that one provider account or integration can affect many customers.

The team documents logical separation, role boundaries, technician assignment, API scope, cross-customer search or scripting capability, logging, and emergency access. It should know whether a global MSP administrator can reach the CMMC customer and under what controls.

Multi-tenancy is not automatically disqualifying. It is a fact that must be understood, controlled, and evidenced.

B.57 MSP Documentation Systems

Documentation platforms can contain network diagrams, IP addresses, firewall rules, credentials or credential references, recovery procedures, configuration details, customer contacts, and security architecture. This information may constitute Security Protection Data even when CUI is intentionally excluded.

The review identifies what is stored, who can access it, authentication, export capability, backup, sharing, retention, technician offboarding, and provider termination.

Where credentials are stored separately in a vault, the documentation system should not quietly recreate the same secret through screenshots or notes.

B.58 Remote Support Session Scoping

Remote support can expose screen content, clipboard data, transferred files, session recordings, chat transcripts, and administrative actions. The MSP identifies which remote tools are approved and what features are enabled.

If sessions can be recorded, the team determines where recordings are stored and whether protected information could be captured. If file transfer is enabled, it defines when and where transferred files may be stored.

Technicians should know how to stop or redirect a session when protected information appears in an unapproved support channel.

B.59 Mobile Administration by MSP Personnel

Administrative access from phones or tablets can create a separate privileged path. The provider determines whether mobile administration is permitted, which applications are used, how devices are managed, whether credentials or tokens persist, and whether screenshots, downloads, or local files are possible.

If mobile administration is prohibited, the technical environment should support that decision rather than relying only on a handbook statement.

Emergency access procedures should not quietly bypass the provider's normal device and identity controls.

B.60 Home-Based MSP Technicians and Distributed Support

A remote technician may administer a customer from a home office while using an MSP-managed endpoint. The analysis focuses on the controlled administrative path: device management, authentication, network connection, privacy from household members, local printing and storage, remote-support tooling, monitoring, and physical handling.

The provider should define whether privileged work can occur from any location or only approved locations and devices. Contractors should understand this service model rather than assuming that 'the MSP's office' is the source of all administration.

After-hours subcontractors and overseas support, if present, require explicit review against contractual, export, data, and service requirements rather than being treated as ordinary staffing.

B.61 Evidence Repositories and Assessment Workspaces

Readiness work often creates a new repository containing screenshots, configurations, policies, inventories, vulnerability reports, logs, diagrams, and interview notes. This repository can become one of the most sensitive collections in the program.

The organization decides where evidence is stored, who can contribute, who can read it, how versions are controlled, how external readiness personnel access it, how assessment evidence is shared, and what is retained after assessment.

Evidence should be protected according to its content. A folder created for compliance should not become an uncontrolled copy of the environment.

B.62 Scope Reduction: What It Means and What It Does Not Mean

Scope reduction is the deliberate architectural effort to limit the systems and people that need to handle or protect CUI. Examples can include a dedicated enclave, controlled VDI, restricted collaboration sites, segmentation, or specialized workflows.

Scope reduction is legitimate when the resulting architecture reflects how work is actually performed. It fails when employees must routinely bypass the boundary to do their jobs or when shared identity, administration, backup, logging, printing, or integration dependencies are ignored.

The objective is not the smallest possible diagram. It is the smallest practical, truthful, defensible environment that supports the business mission.

B.63 Enclave Design and MSP Responsibilities

In an enclave model, the MSP helps define the boundary between protected and ordinary business systems. The team maps identity, endpoints or VDI, network segmentation, cloud services, printing, external exchange, administration, monitoring, backup, and support.

An enclave does not eliminate shared services automatically. If a shared identity platform, RMM, backup system, or administrator can materially affect the enclave, that dependency must be analyzed.

The contractor also needs a business process that keeps CUI inside the enclave. Technical segmentation cannot compensate for a workflow that requires employees to copy information into ordinary corporate systems.

B.64 MSP Onboarding as a Scoping Event

When a new MSP begins service, the contractor should treat onboarding as a scope-changing project. The MSP introduces agents, administrative accounts, delegated roles, portals, integrations, scripts, backup relationships, monitoring, documentation, and technician access.

Before deployment, the parties record what each tool does and whether it handles CUI, Security Protection Data, or privileged administration. After deployment, diagrams, inventories, responsibility matrices, and the SSP are updated.

This turns MSP onboarding from an invisible technical change into a controlled architectural event.

B.65 Customer Onboarding From the MSP Perspective

The MSP should maintain a CMMC-specific onboarding track for customers with protected environments. Sales and account management identify the customer's contractual context early enough that engineering does not deploy the ordinary stack without review.

Engineering then performs discovery, documents existing providers and privileged paths, identifies inherited weaknesses, and separates assumptions from verified facts. Security personnel determine monitoring and escalation. Documentation owners establish evidence retention and responsibility records.

The MSP should not promise that its standard stack 'makes the customer CMMC compliant.' It should describe the specific capabilities and operational responsibilities the service provides.

B.66 Customer Offboarding From the MSP Perspective

Offboarding closes technical and evidence relationships. The MSP inventories customer data and security information in its systems, exports or transfers agreed documentation and evidence, removes agents and integrations, revokes accounts and tokens, closes delegated administration, handles retained backups according to contract, and verifies that technicians can no longer reach the customer.

Evidence of offboarding should be retained according to the parties' requirements. The contractor should confirm receipt of necessary historical material before provider access disappears.

A clean exit is part of security architecture, not merely contract administration.

B.67 Acquisitions, Divestitures, and Corporate Restructuring

Corporate transactions can change ownership, networks, identity, facilities, personnel, providers, and information flows quickly. The CMMC program should be included in technical due diligence before systems are merged.

A newly acquired company should not be connected to the protected environment simply because both organizations now share ownership. The team evaluates the target environment, intended CUI workflows, administrative access, and integration plan.

Divestiture requires the reverse analysis: data separation, account removal, provider changes, evidence retention, and updates to the assessment boundary.

B.68 Incident Response Can Reveal Hidden Scope

Cyber incidents often expose connections that diagrams missed. An investigation may discover a forgotten admin tool, an unmanaged file copy, an old VPN account, a vendor tunnel, a shadow SaaS service, or logs forwarded to an unknown destination.

After an incident, the organization should compare investigation findings with the documented scope. New facts trigger updates to inventories, diagrams, responsibility matrices, and risk decisions.

The incident response process therefore serves as a continuous validation mechanism for scoping.

B.69 Discovery Techniques for Finding Hidden Assets and Flows

Scoping should combine interviews with technical discovery. Useful sources can include identity directories, device management, RMM, EDR, vulnerability scanners, DHCP/DNS, firewall rules, network discovery, cloud inventories, SaaS administration, backup inventories, authentication logs, email-flow information, application lists, procurement records, and support tickets.

No single tool should be treated as the authoritative truth. Differences between inventories are findings to reconcile.

The readiness team documents the date and method of discovery so the resulting inventory can be repeated and maintained.

B.70 Sampling Does Not Replace Inventory

Assessment activities may use sampling under applicable guidance, but the organization still needs to understand the full asset population required by the current scoping rules. Sampling is not a shortcut for an incomplete inventory.

The MSP should be able to reconcile agent-based tools against the authoritative asset population and explain legitimate exclusions. If 150 protected endpoints exist but

only 142 appear in EDR, the missing eight require investigation rather than a percentage-based declaration of success.

B.71 Scoping Decisions Need Evidence

Consequential scope decisions should have a short written rationale tied to facts. If a service is considered out of scope, document the architecture and controls supporting that conclusion. If a platform is a Security Protection Asset, identify the security function it provides. If a cloud provider stores CUI, document the applicable provider requirements and supporting evidence.

These decision records reduce repeated debate and help future teams understand why the boundary was designed a particular way.

A decision record should be revisited when its underlying facts change.

B.72 Scoping Assumptions Register

Not every question can be answered on the first day. The team should maintain an assumptions register rather than converting uncertainty into a permanent architecture statement.

Each assumption records the question, current working assumption, business impact, technical impact, owner, authoritative source needed, due date, and resulting scope change if the assumption proves false.

This is especially useful for prospective contractors designing an environment before final contract data flows are known.

B.73 Scope Change Control

Once the boundary is established, ordinary change management should include a CMMC scope-impact question. A new SaaS application, firewall rule, integration, backup target, admin tool, subcontractor, remote-access method, facility, or workflow can alter the assessment story.

The change record need not become a compliance essay. It should identify whether CUI flow, Security Protection Data, privileged access, provider relationships, asset category, SSP content, diagrams, or evidence are affected.

Material changes are escalated to the CMMC program owner for documented review.

B.74 Scoping Review Cadence

Scope is reviewed on a schedule and on triggering events. Periodic review catches gradual drift; event-driven review catches major changes immediately.

The review compares current asset and identity inventories, provider lists, diagrams, data flows, and responsibility records. It also samples real tickets and recent changes to test whether documentation still reflects operations.

The organization should be able to state when the scope was last reviewed, who participated, what changed, and what evidence supported the review.

B.75 Comprehensive MSP Scoping Interview Questions

The final interview should force concrete answers. What systems can your technicians reach? From what devices? Through what portals? Can you transfer files? Can you view customer screens? Can you run scripts? Where are logs stored? Where are backups stored? Which subcontractors can access the service? What happens after hours? What happens if a global administrator is compromised? What customer information enters tickets? What is in your documentation platform? What APIs connect your tools? How are departed technicians removed?

The same interview asks what the MSP cannot do. Which systems are customer-managed? Which applications require a separate vendor? Which security functions are outside the MSP agreement? Who owns physical controls? Who owns employee screening? Who approves access? Who owns incident reporting to DoD?

Clear limitations are as important as clear capabilities because they prevent responsibility gaps.

B.76 Comprehensive Scope Decision Matrix

Object / Service	Business Function	CUI Relationship	Security Function / SPD	Admin Capability	External Provider	Proposed Treatment	Evidence / Rationale	Change Trigger
Identity platform								
User endpoint class								
MSP technician endpoint								
RMM								

PSA/ ticketing								
Credential vault/PAM								
EDR								
Vulnerability management								
SIEM/SOC								
Backup								
Firewall/ VPN								
Email security gateway								
Microsoft collaboration								
SaaS/file exchange								
Engineering/ CAD								
ERP/business app								
DevOps/ repository								
Printer/MFD								
OT/test/ specialized asset								
Evidence repository								

B.77 Provider Dependency Matrix

Provider	**Service**	**CUI?**	**Security Protection Data?**	**Privileged Access?**	**Subprocessors / Subcontractors**	**Contract / Responsibility Evidence**	**Exit Plan**
MSP							
Cloud Service Provider							
SOC/MSSP							

Backup Provider							
RMM Vendor							
PSA Vendor							
Security Platform Vendor							
Specialized Implementer							

B.78 Scope Validation Walkthrough

Before declaring the boundary ready, select representative workflows and perform them. Receive a protected file. Open it. Edit it. Share it internally. Send it through an approved external path. Back it up. Restore it. Print it if printing is allowed. Generate security telemetry. Open a support ticket. Perform an MSP administrative action. Offboard a test identity. Then compare every system and provider observed during the walkthrough with the documented scope.

Repeat the walkthrough from the MSP side. Have a technician connect from the approved source device, authenticate, retrieve any necessary privileged credential, administer the customer, create a ticket, escalate to another engineer, and close the work. Observe what platforms received data and what logs were created.

A discrepancy between the walkthrough and the diagram is more valuable before assessment than a perfectly formatted diagram that no longer represents reality.

B.79 Final Comprehensive Management Gate

Management Question	**Verified**	**Evidence**	**Owner**	**Decision / Follow-up**
Can we explain the contract-driven reason for the protected environment?				
Can we trace representative CUI from creation/receipt through destruction?				
Can we trace MSP privileged administration from technician device to customer asset?				
Can we trace security telemetry from source to monitoring and evidence?				

Have all relevant asset categories been assigned using current DoD guidance?				
Have all ESP/CSP relationships been analyzed service by service?				
Do we know where every relevant backup, log, ticket, and evidence copy resides?				
Can we identify every non-human privileged identity and integration?				
Can we explain shared MSP platforms and tenant separation?				
Have remote technicians, subcontractors, and after-hours support been evaluated?				
Do diagrams, inventory, SSP, responsibility matrix, and live operation agree?				
Can we detect when the scope changes?				
Can we exit or replace a provider without losing control or evidence?				
Have consequential scoping decisions been documented with rationale?				
Have current official CMMC scoping resources been checked before the final decision?				

B.80 Final Comprehensive Teaching Standard

A comprehensive MSP scope is not a list of products and it is not a declaration that the entire provider is either inside or outside the customer's CMMC environment. It is a documented explanation of how the contractor performs protected work, how information moves, how the environment is administered, how security protections are delivered, and where external providers participate.

The contractor should be able to point to every material service relationship and explain why it matters or why it does not. The MSP should be able to identify its relevant people, platforms, privileged paths, data, security functions, and

subcontractors. The readiness specialist should be able to trace those facts to current guidance without changing the facts to obtain a preferred boundary.

When those three perspectives agree—and the live walkthrough confirms the documentation—the organization has a scope that is practical enough to operate, detailed enough to assess, and durable enough to maintain.

B.81 Final Completeness Check: What Was Still Missing

The final completeness review found that the comprehensive draft covered the major MSP tools and provider relationships well, but several boundary subjects deserved explicit treatment before this appendix could be frozen. These were physical separation and logical separation, boundary components, security appliances that serve both protected and ordinary networks, temporary systems, test and staging environments, disaster-recovery environments, data migration, inherited legacy systems, Government-furnished systems, shared corporate services, provider incident-response evidence, and the distinction between scoping evidence and assessment evidence.

Adding these subjects matters because scope is usually challenged at the seams. The obvious CUI file server is rarely the hardest question. The difficult questions involve a shared identity system, an administrator's laptop, a temporary migration tool, a disaster-recovery copy, a security appliance that protects several networks, or a provider platform whose role changes depending on the service delivered.

B.82 Physical Separation Versus Logical Separation

An organization can separate a protected environment physically, logically, or through a combination of both. Physical separation may use dedicated networks, devices, and facilities. Logical separation may use segmentation, tenant boundaries, virtual networks, access-control policy, identity restrictions, and other technical controls.

Neither approach should be accepted merely because a diagram draws a boundary. The team verifies how the separation is enforced and how administration crosses it. A shared hypervisor, identity service, backup platform, firewall, management plane, or privileged administrator can create dependencies across an otherwise clean-looking boundary.

The correct question is therefore not whether the environment has its own VLAN or tenant. The question is whether the complete architecture and operating procedures support the proposed scoping treatment.

B.83 Boundary Components and Shared Security Infrastructure

Firewalls, gateways, identity systems, DNS, security appliances, management networks, jump hosts, bastions, proxies, and other boundary components can provide protection to the assessed environment while also serving ordinary corporate systems.

The scoping team identifies the specific capability that supports the protected environment and determines how the current CMMC asset-category rules apply. Shared infrastructure should not be hidden simply because only part of its traffic relates to CUI.

Where feasible, separation can simplify administration and evidence. Where shared infrastructure remains necessary, configuration, access, logging, change control, and responsibility must be clearly documented.

B.84 Jump Hosts, Bastions, and Privileged Access Workstations

A jump host or privileged access workstation can deliberately constrain administrative access. The design should identify who can reach the administrative platform, from which source devices, how authentication occurs, what destinations are permitted, whether files and clipboard data can move through it, and what actions are logged.

These systems can reduce uncontrolled privileged paths, but they become important security components themselves. Their configuration, patching, monitoring, access review, and recovery therefore require explicit ownership.

The MSP should demonstrate the actual administrative workflow rather than presenting the jump host as an architectural symbol.

B.85 Temporary, Staging, Migration, and Project Systems

Temporary systems are easy to omit because the team assumes they will disappear before assessment. Migration servers, file-transfer staging areas, discovery appliances, consultant laptops, test tenants, temporary VPNs, project shares, and data-conversion tools can nevertheless process CUI or provide privileged access while they exist.

The project plan should identify temporary assets before deployment, define their approved use, protect them according to the function they perform, and establish a removal date and closure test.

At project completion, the organization verifies that temporary accounts, data copies, firewall rules, agents, API keys, and storage have actually been removed or transitioned.

B.86 Development, Test, QA, and Staging Environments

A non-production label does not make an environment irrelevant. Test systems may contain production copies, CUI-derived data, configuration exports, credentials, security tooling, or administrative connectivity to production.

The preferred design minimizes protected information in development and test unless it is required. When representative data can be synthesized or de-identified appropriately, that may reduce unnecessary exposure. When real protected information is necessary, the environment is analyzed according to its actual use.

Developers and vendors often have broader privileges in non-production environments, making accurate data classification and access control especially important.

B.87 Disaster Recovery and Alternate Processing Environments

Disaster-recovery systems can become forgotten copies of the production scope. Replicated virtual machines, standby databases, alternate cloud regions, recovery networks, offline media, and warm or cold sites should be mapped according to the information and security functions they contain.

The organization determines who can activate the environment, how identities and security controls function during recovery, how monitoring continues, and how evidence is preserved.

A recovery environment that is secure only after someone remembers to configure it during an emergency is not a mature design.

B.88 Data Migration and Bulk Transfer

Moving into or out of a protected environment can create one of the largest temporary CUI flows in the program. Migration tools may stage data, create exports, use temporary cloud storage, employ vendor personnel, or generate logs containing sensitive paths and metadata.

The migration plan identifies source, destination, transfer mechanism, temporary storage, encryption, privileged identities, validation, rollback, deletion, and evidence. Specialized implementers are included in the provider map.

After migration, the team verifies both successful transfer and cleanup of intermediate copies.

B.89 Legacy Systems and Unsupported Technology

Legacy systems can remain operational because a contract, manufacturing process, laboratory device, or engineering application depends on them. The scoping team records why the system exists, what information it handles, how it connects, who maintains it, and what limitations affect implementation.

The organization should not hide a legacy system from scope because it is difficult to secure. Instead, it documents the real architecture and evaluates the applicable requirements, risk, isolation, maintenance, and modernization path.

The MSP should clearly identify where ordinary patching or endpoint tooling cannot be applied so management understands the operational constraint.

B.90 Government-Furnished Equipment and Government Systems

Government-furnished equipment can participate directly in the contractor's workflow while ownership remains with the Government. The organization documents where the equipment is located, what information it handles, how it connects, who administers it, and which party is responsible for each security function.

The same care applies when contractor personnel access Government systems. The contractor should distinguish the Government system from the contractor systems and endpoints used to reach it.

Ownership alone does not answer the scoping question; function, information, connectivity, and responsibility do.

B.91 Shared Corporate Services

Organizations frequently want to exclude corporate services such as HR, finance, identity, help desk, procurement, or enterprise management from the protected environment. That may be appropriate for some services, but the decision must follow actual data and security dependencies.

If a corporate help desk can reset privileged accounts, if enterprise identity authenticates protected users, or if a corporate management tool can execute commands on protected endpoints, the relationship must be analyzed.

Scope reduction works only when shared services are either genuinely separated from protected functions or accurately included according to their role.

B.92 DNS, NTP, PKI, Certificate Services, and Foundational Dependencies

Foundational infrastructure is often omitted because it does not look like a business application. DNS supports name resolution, time services support trustworthy event correlation, and PKI or certificate services may support authentication, encryption, device trust, VPN, or administrative connections.

The team identifies which foundational services the protected environment relies upon, who operates them, how they are secured, and what happens if they fail or are compromised.

The scoping treatment should follow the security capability actually provided and current asset-category guidance.

B.93 Email Security, DLP, Web Filtering, and Security Gateways

Security gateways may sit outside the main collaboration tenant while providing protection to it. Email filtering, secure web gateways, DNS filtering, DLP, CASB/SSE services, and similar technologies can receive message metadata, content, security telemetry, or policy information.

The team maps data inspection, storage, administration, logs, provider access, integrations, and security function. If the service processes CUI, that fact is evaluated directly. If it provides a security protection capability without CUI, Security Protection Asset analysis may apply.

Marketing labels such as 'security cloud' or 'zero trust service' do not replace this functional analysis.

B.94 Incident Response Providers, Forensics, and DFARS Evidence Preservation

An incident can expand the set of organizations temporarily handling highly sensitive information. Forensics providers may receive disk images, memory captures, logs, malware samples, account data, and copies of affected information.

DFARS 252.204-7012 requires rapid cyber-incident reporting when the clause applies and requires preservation and protection of images of affected systems and relevant monitoring or packet-capture data for at least 90 days from submission of the report. It also imposes obligations relating to malicious software and access to information needed for forensic analysis.

The incident-response plan should therefore pre-identify how MSP, MSSP, forensic provider, contractor management, and legal/contract functions coordinate without creating uncontrolled evidence transfers. Provider incident workflows belong in the service-dependency map.

B.95 Cloud Provider Incident and Forensic Obligations

When an external cloud service provider stores, processes, or transmits covered defense information under DFARS 252.204-7012, the contractor must require and ensure that the provider meets security requirements equivalent to the FedRAMP Moderate baseline and complies with specified incident reporting, malicious-software, media-preservation, forensic-access, and damage-assessment obligations.

This means cloud-provider selection is not solely a feature or encryption decision. The contractor needs evidence supporting the applicable service commitments and must understand how incident information will be obtained when needed.

The MSP can help collect provider documentation and design the service, but the contractor remains responsible for ensuring the contractual requirement is addressed.

B.96 Subcontractor Versus MSP Provider Chains

A subcontractor performing part of the DoD work and an MSP providing technology services may both be external organizations, but their contractual roles are different. A subcontractor may receive CUI because it performs part of the covered work. An MSP may receive CUI or Security Protection Data because it operates the contractor's systems. Some organizations may perform both kinds of functions.

The contractor should therefore maintain both a supply-chain flow map and a service-provider map. Where the same company appears in both, the responsibilities should be documented separately.

This distinction helps prevent a technology service agreement from being mistaken for the complete flowdown analysis required for subcontract performance.

B.97 COTS Exceptions Do Not Create a General Technology Exemption

Current DFARS applicability provisions contain exceptions for solicitations or contracts solely for commercially available off-the-shelf items. That contracting exception should not be confused with a rule that ordinary commercial technology

used inside a covered contractor information system is automatically outside the security boundary.

The scoping analysis continues to follow the covered work, information, systems, and security functions. Commercial availability of a laptop, firewall, SaaS product, or application does not by itself determine its CMMC asset category.

This distinction is useful when business teams encounter the term COTS in contract language and mistakenly apply it to internal asset scoping.

B.98 Evidence Needed to Support a Scope Decision

Every major scope decision should be supported by evidence proportionate to its consequence. Useful evidence can include data-flow diagrams, network diagrams, system inventories, identity exports, tool coverage reports, provider service descriptions, customer responsibility matrices, contracts, configuration records, screenshots, interviews, architecture decisions, and technical tests.

The evidence should establish the factual basis for the decision rather than merely repeat the conclusion. A document saying 'PSA is out of scope' is weaker than a documented workflow showing that CUI is prohibited, technicians use an approved alternative, ticket samples and configuration support that practice, and the remaining Security Protection Data relationship has been separately evaluated.

Appendix D will organize evidence in greater depth, but scoping cannot wait until Appendix D to become evidence-based.

B.99 Scope Evidence Versus Control Evidence

Scope evidence answers questions such as what assets exist, what data flows through them, which provider operates them, and why they are categorized a certain way. Control evidence answers whether an applicable security requirement is implemented and operating.

The two overlap but are not identical. An RMM inventory may help establish which endpoints exist and also help demonstrate configuration or maintenance activities. A provider agreement may support the service boundary but not prove that MFA is operating.

Keeping the distinction clear helps the assessment team avoid using a contract statement as proof of a technical control or using a single screenshot as proof of the entire boundary.

B.100 Negative Testing of the Proposed Boundary

A strong scoping exercise tries to disprove its own assumptions. If the design says ordinary corporate laptops cannot reach the protected environment, test that claim. If CUI cannot enter the PSA, test the workflow and technical controls. If only managed technician endpoints can administer the tenant, attempt access from an unmanaged device under controlled conditions.

Negative testing should be authorized and carefully planned, but it provides valuable evidence that separation is real rather than conceptual.

When a negative test succeeds unexpectedly, the team updates the architecture and scope before relying on the original boundary.

B.101 Walkthrough: A CUI Email From Prime Contractor to Engineer

A prime contractor sends a protected technical attachment to an engineer. The team traces the message through the mail provider and any security gateway, into the engineer's mailbox, onto the approved endpoint or controlled session, and into the approved project repository. It identifies backup, journaling, mobile access, external forwarding, and administrator visibility.

The MSP then traces the security path: identity authentication, device compliance, EDR telemetry, mail-security events, SIEM forwarding, and administrative support. Every service observed is compared with the scope and provider map.

This one workflow can reveal more about the true environment than a long product inventory.

B.102 Walkthrough: MSP Administrator Responds to a Security Alert

The SOC detects suspicious activity on a protected endpoint and opens an incident. The MSP technician authenticates from an approved administrative device, uses the approved privileged path, reviews EDR telemetry, isolates the endpoint if authorized, records actions in the ticketing or case system, and escalates according to the incident plan.

The walkthrough identifies every provider, platform, identity, log, and evidence repository involved. It also checks whether the ticket or case system receives CUI or only security information.

The contractor then verifies that its own incident and contractual reporting decision process begins at the correct handoff.

B.103 Walkthrough: Engineering File Sent to a Subcontractor

The contractor determines that a subcontractor requires a protected engineering file to perform covered work. Contracts personnel verify the applicable flowdown and status requirements. The business owner authorizes the recipient. The file is transmitted through the approved protected exchange method.

The MSP demonstrates the technical transfer path and logging. The contractor records the subcontractor relationship and the information released. If another cloud or transfer provider participates, that service appears in the information-flow map.

This walkthrough connects supply-chain governance with technical scope instead of treating them as separate programs.

B.104 Walkthrough: MSP Tool Vendor Suffers an Incident

Assume the MSP's RMM, documentation, backup, or security-platform vendor reports a compromise. The MSP identifies whether the affected service can reach the contractor, what credentials or tokens are exposed, what customer information or Security Protection Data may be affected, and what containment is possible.

The contractor evaluates its own incident and contractual obligations using verified facts. Privileged credentials, API keys, agents, or integrations may need to be revoked or changed. Evidence is preserved.

The event also tests whether the provider chain was documented before the emergency. If the contractor first learns the name of the upstream vendor during the incident, provider governance was incomplete.

B.105 The Scoping Challenge Review

Before freezing the boundary, assign a knowledgeable person who did not design it to challenge the assumptions. That reviewer asks where CUI could escape, what shared service was overlooked, which administrator has a path that is not shown, which provider receives telemetry, where temporary copies appear, what happens during recovery, and which workflow employees bypass when under pressure.

The objective is not to make scope larger. It is to make scope truthful. A defensible exclusion is valuable; an exclusion based on an untested assumption is a future finding.

Results of the challenge review are documented as confirmed decisions, corrections, or open questions.

B.106 Final Completeness Checklist

Completeness Question	Verified	Evidence / Rationale	Owner	Action
Have contract and business-process drivers been traced into technical scope?				
Have physical and logical separation mechanisms been validated?				
Have shared boundary/security components been evaluated?				
Have jump hosts and privileged access workstations been mapped?				
Have temporary, staging, migration, test, and QA systems been evaluated?				
Have DR, replication, alternate processing, and recovery copies been mapped?				
Have legacy and unsupported systems been addressed truthfully?				
Have GFE and Government-system access paths been documented?				
Have shared corporate identity/help-desk/management services been evaluated?				
Have DNS, NTP, PKI, certificate, and foundational dependencies been considered?				
Have email/DLP/web-security gateways been evaluated by function and data?				
Are incident-response/forensics providers included in provider mapping?				

Are DFARS cloud-provider incident/forensic obligations addressed where applicable?				
Are subcontractor work-performance flows separated from MSP service-provider analysis?				
Have COTS contracting exceptions been kept distinct from internal asset scoping?				
Does every consequential scope decision have factual evidence and rationale?				
Are scope evidence and control evidence distinguished?				
Has the proposed boundary been negatively tested where practical?				
Have representative CUI, MSP-admin, SOC-response, and subcontractor workflows been walked end to end?				
Has an independent internal challenge review attempted to find hidden dependencies?				
Do the live environment, diagrams, SSP, inventory, provider map, and responsibility matrix agree?				
Has the team rechecked the current official DoD CMMC Level 2 Scoping Guide before assessment?				

B.107 Final Appendix B Standard

Appendix B is complete when a contractor and its MSP can sit together with the system diagram, asset inventory, provider map, responsibility matrix, and live administrative tools and tell the same story. The story begins with the covered work and CUI, follows the user and data paths, follows privileged administration, follows security telemetry, identifies every consequential external dependency, and explains the evidence supporting each scope decision.

The final boundary should survive three tests. It should survive a technician walkthrough, because the documented path must match how the system is actually operated. It should survive a failure scenario, because backup, incident response, provider compromise, and disaster recovery can expose dependencies hidden during normal operation. And it should survive an independent challenge, because an assessor should not be the first person to discover that a supposedly excluded system can administer, protect, store, or transmit information for the assessed environment.

With these additions, Appendix B provides the bridge from the broad readiness model in Appendix A to the detailed responsibility, evidence, SSP, POA&M, assessment, technician, onboarding, incident, cross-reference, glossary, and continuous-readiness tools that follow in the remaining appendices.

CMMC for MSPs: From Readiness to Certification

Appendix C
Sample Responsibility Matrix

Final Teaching Edition

Authored by Dr. Charles Edwards

C.1 Purpose of This Appendix

A CMMC responsibility matrix is the operating agreement that connects cybersecurity requirements to real people, real services, real systems, and real evidence. It answers a deceptively simple question: when a requirement must be satisfied every day, who is actually responsible for making that happen? In a small contractor, the answer may involve one internal administrator. In a modern defense contractor supported by an MSP, cloud provider, security operations provider, backup vendor, readiness specialist, and other subcontractors, the answer is usually distributed across several organizations.

The matrix is therefore not a compliance decoration. It is a control-management instrument. It should be detailed enough that a contractor executive can understand accountability, an MSP technician can understand assigned operational duties, a readiness specialist can identify gaps, and an assessor can trace statements in the System Security Plan to the people and systems that perform the work.

This appendix teaches how to build, validate, use, and maintain that matrix. The sample tables at the end are intentionally more detailed than a conventional RACI chart because CMMC responsibilities cannot be reduced safely to a single letter in every row.

C.2 Current CMMC Context for Responsibility Allocation

Responsibility allocation must begin with the contract and the current CMMC requirement, not with a generic checklist. Under the current DFARS framework, a solicitation can specify CMMC Level 1 (Self), Level 2 (Self), Level 2 (C3PAO), or Level 3 (DIBCAC). Where the CMMC clause applies, the contractor must have and maintain the required current status for the contractor information systems used in performance that process, store, or transmit FCI or CUI. The contractor also has annual affirmation responsibilities and flowdown obligations when applicable. These obligations make the contractor the central accountable organization even when technical work is outsourced.

The practical consequence is important: an MSP can operate identity, endpoints, firewalls, backups, logging, vulnerability management, or other services, but the contractor still needs to know what is being done, what evidence proves it, what contractual commitments support it, and whether the combined environment satisfies the applicable requirement. Outsourcing operation does not erase contractor accountability.

For Level 2 scoping, the DoD scoping guidance also recognizes External Service Provider relationships. When an ESP meets the applicable CUI Asset or Security Protection Asset criteria, the relationship and services need to be documented in the organization seeking assessment's SSP, and the provider's service description and customer responsibility matrix become important sources for allocating responsibility. This makes responsibility documentation part of the architecture and evidence story, not merely an administrative exercise.

C.3 The Multi-Party CMMC Operating Model

The most useful way to think about a CMMC environment is not as a three-party relationship but as a chain of accountability, implementation, operation, evidence, and independent evaluation. The defense contractor or offeror owns the business decision to pursue or perform the DoD work and remains accountable for its CMMC obligations. The MSP or other ESP performs the technical and operational services assigned by contract. A readiness or compliance specialist may help interpret requirements, build documentation, organize evidence, and identify gaps. Specialized providers may operate cloud, SOC, backup, email security, vulnerability, or other services. A C3PAO, where a Level 2 C3PAO assessment is required, independently assesses rather than becoming part of the implementation team.

		These roles should never be blurred. A readiness consultant may help the contractor prepare, but preparation is not independent certification. An MSP may generate evidence, but evidence generation is not the same as contractor approval. A cloud provider may supply

		platform capabilities, but platform capability does not automatically satisfy the contractor's complete requirement. A C3PAO may evaluate implementation, but it should not be treated as the contractor's outsourced compliance department.

Party

Primary Role

What the Matrix Must Clarify

Defense Contractor / Offeror

Accountable organization

Business ownership, approvals, contract interpretation, scope, SSP ownership, affirmations, evidence acceptance, provider oversight.

MSP / MSSP / ESP

Assigned technical operator

Exact systems and services operated, privileged access, monitoring, maintenance, incident duties, evidence supplied, escalation.

Readiness / Compliance Specialist

Preparation and coordination support

Requirement interpretation support, gap analysis, documentation assistance, evidence organization, readiness validation.

Specialized Provider / CSP / SOC / Backup / SaaS

Service-specific provider

Provider boundary, inherited/shared functions, service commitments, logs, configuration, incident and evidence interfaces.

C3PAO when applicable

Independent assessor

Assessment activities only; evaluates evidence and implementation rather than owning contractor operations.

C.4 Seven Questions for Every Responsibility

A conventional RACI matrix asks who is Responsible, Accountable, Consulted, and Informed. That model is useful, but it is too compressed for many CMMC operating relationships. A stronger CMMC matrix asks seven questions for every requirement or operational activity: who owns the obligation, who makes the decision, who implements the mechanism, who operates it after implementation, who produces evidence, who maintains or retains that evidence, and who independently assesses it when an independent assessment applies.

		Separating implementation from operation is especially important. A specialized Microsoft provider may build a GCC High tenant, but the MSP may operate users, devices, Conditional Access, Defender, and support after migration. Separating evidence production from evidence ownership is equally important. An MSP may export an EDR policy report, but the contractor should know where the approved evidence package is retained and who can explain it during an

		assessment.

Question

Meaning

Typical Failure if Unclear

Who owns it?

Who is accountable for the obligation and outcome?

Everyone assumes the provider owns compliance.

Who decides?

Who approves architecture, risk, exceptions, or policy?

Technicians make unapproved compliance-impacting decisions.

Who implements?

Who initially configures or deploys the control?

Implementation is assumed but never assigned.

Who operates?

Who performs recurring work after go-live?

A control works at assessment preparation but decays later.

Who produces evidence?

Who creates reports, tickets, logs, screenshots, records?

Evidence is unavailable even though the technology exists.

Who maintains evidence?

Who retains, organizes, and protects evidence?

Evidence is scattered across vendor portals and mailboxes.

Who assesses?

Who independently evaluates where required?

Readiness support is confused with independent assessment.

C.5 Accountability Cannot Be Outsourced

The contractor may outsource many technical functions, but it cannot safely outsource awareness of its own environment. The contractor should be able to explain which information systems process, store, or transmit FCI or CUI; which providers support those systems; which provider responsibilities are inherited or shared; what

evidence demonstrates performance; and how failures are escalated. This is the practical meaning of retaining accountability while outsourcing operations.

This distinction protects both parties. It prevents the contractor from saying, “the MSP handles CMMC,” which is too broad to be operationally meaningful. It also prevents the MSP from accepting undefined liability for business decisions, contract interpretation, personnel actions, physical security, training, policy approval, or other responsibilities outside the managed-services scope.

C.6 Start With the Contract, Scope, and Service Agreements

Responsibility mapping should be built from four sources at the same time: the solicitation or contract requirement, the CMMC assessment scope, the SSP and supporting procedures, and the actual provider agreements such as the MSA, SOW, service description, SLA, and customer responsibility matrix. If these sources disagree, the disagreement is itself a readiness finding.

For example, an SSP may state that the MSP reviews security alerts daily, while the SOW provides only business-hours monitoring. A responsibility matrix should expose that conflict immediately. Likewise, a contractor may assume the backup provider performs restore testing, while the provider contract only guarantees backup job execution. The matrix forces the organization to convert assumptions into explicit assignments.

C.7 Existing DoD Contractor Scenario

An existing defense contractor begins with reality. The organization may already possess CUI, already use an MSP, already have remote users, already share files with subcontractors, and already operate cloud and security tools. The responsibility workshop should therefore begin by tracing current CUI flows and current administrative paths, then comparing those facts with the contract, SSP, provider agreements, and existing evidence.

The workshop should ask what the MSP actually does today, not what everyone believes the MSP does. Review tickets, admin portals, security reports, backup jobs, patch reports, identity changes, firewall configurations, incident records, and recurring meeting notes. If a responsibility cannot be connected to an observable activity and evidence source, it is not yet a dependable responsibility assignment.

C.8 Prospective DoD Contractor or Offeror Scenario

A prospective contractor has a different advantage: it can design responsibility before CUI enters the environment. The organization should review the solicitation, determine the required CMMC level and assessment type, design the intended CUI environment, choose providers, assign responsibilities contractually, implement the environment, build the SSP and procedures, collect evidence, and validate readiness before relying on that environment for the opportunity.

This scenario is where the responsibility matrix becomes an architecture tool. If the organization knows it lacks internal security operations capability, the matrix can identify that need before selecting a SOC provider. If the MSP does not support GCC High or a required endpoint configuration, the gap can be addressed before migration. Responsibility design therefore belongs early in the program, not only before assessment.

C.9 Responsibility Categories

C.9.1 Governance and Contractual Responsibility

Includes contract review, CMMC level/status interpretation, scope approval, provider selection, risk acceptance, policy approval, annual affirmation, subcontractor flowdown, and executive oversight. These functions normally remain contractor-led even when advisors assist.

C.9.2 Technical Implementation Responsibility

Includes tenant configuration, endpoint enrollment, firewall rules, EDR deployment, logging integration, backup configuration, vulnerability scanners, privileged-access tooling, encryption configuration, and other mechanisms.

C.9.3 Recurring Operational Responsibility

Includes onboarding and offboarding, patching, alert triage, vulnerability remediation, backup monitoring, restore testing, account reviews, firewall reviews, incident handling, log review, and change management.

C.9.4 Documentation Responsibility

Includes the SSP, policies, procedures, diagrams, inventories, data-flow descriptions, provider descriptions, responsibility matrices, incident procedures, and configuration standards.

C.9.5 Evidence Responsibility

Includes generating, validating, retaining, protecting, indexing, and presenting evidence. Evidence responsibility must be explicit because many managed services create evidence inside provider-controlled portals.

C.9.6 Independent Assessment Responsibility

Where a C3PAO assessment is required, the assessor evaluates the environment independently. The matrix may show the C3PAO as assessor for the assessment activity, but should not assign it operational control ownership.

C.10 Responsibility Assignment by Technology and Service

C.10.1 Identity, Accounts, and MFA

The contractor decides who should have access and approves business roles. The MSP may create accounts, enforce MFA, configure Conditional Access, maintain privileged groups, and produce access reports. HR or management must still communicate hires, terminations, transfers, and role changes. The matrix must show the handoff from personnel decision to technical execution and then to evidence.

C.10.2 Microsoft 365 Government, GCC, and GCC High

Microsoft government cloud environments are service platforms, not a compliance result by themselves. A specialized provider may establish or migrate the tenant; the MSP may operate identity, Exchange, SharePoint, OneDrive, Teams, Defender, device management, and support; the contractor approves architecture, data use, external sharing, and business access. The matrix should identify tenant ownership, licensing, privileged roles, configuration baselines, change approval, service health monitoring, evidence exports, and incident escalation.

C.10.3 Endpoint Management and Hardening

The contractor defines which devices are authorized for CUI work. The MSP may enroll devices, apply baselines, configure encryption, deploy security agents, patch systems, and monitor health. The responsibility matrix should also state who handles exceptions, unsupported devices, local administrator requests, lost devices, and devices that stop reporting.

C.10.4 EDR and Endpoint Security

The provider may deploy and operate EDR, but the matrix must distinguish policy ownership, agent deployment, health monitoring, alert triage, containment authority,

escalation, investigation, and evidence retention. A green dashboard is not enough if nobody is assigned to act on alerts or missing agents.

C.10.5 RMM

RMM creates powerful privileged administration paths. The matrix should identify who administers the RMM platform, who approves technicians, how MFA and privileged access are enforced, how scripts are controlled, how sessions are logged, how customer separation is maintained, and what happens if the RMM vendor or MSP is compromised.

C.10.6 PSA and Ticketing

Ticket systems may contain security data and can accidentally receive CUI. The matrix should identify ticket-content rules, access control, retention, attachments, escalation, integration with RMM, evidence generation, and procedures when CUI is placed into an unapproved ticketing platform.

C.10.7 SIEM, SOC, and MSSP

Logging responsibility has at least four layers: log generation, transport, retention, and review/response. The endpoint or system owner may generate logs; an MSP may configure forwarding; a SIEM provider may retain them; a SOC may monitor and escalate. The contractor needs one coherent assignment across all four layers.

C.10.8 Vulnerability and Patch Management

Scanning, prioritization, remediation, exception approval, patch deployment, validation, and evidence are different duties. A scanner vendor does not remediate vulnerabilities. An MSP that patches operating systems may not patch specialized engineering applications. The matrix must expose these boundaries.

C.10.9 Backup and Recovery

The matrix should distinguish backup configuration, encryption, monitoring, failure response, retention, immutability where used, restore testing, business recovery priorities, and evidence. The contractor decides recovery objectives; the provider may operate the technology. Successful backup jobs do not prove successful restoration.

C.10.10 Firewalls, VPN, and Network Security

Assign rule approval, implementation, review, firmware maintenance, VPN access, remote administration, configuration backup, log forwarding, and emergency changes. The contractor should know which changes require business approval and which operational changes the MSP may make under standing authority.

C.10.11 Incident Response

The contractor owns the organizational incident-response obligation. The MSP may detect, contain, preserve evidence, investigate assigned systems, and provide technical facts. Legal, contractual, reporting, executive, customer, and law-enforcement decisions may belong elsewhere. The matrix must define who can isolate systems and who makes external reporting decisions.

C.10.12 Physical Security and Media

MSPs often have limited visibility into facility access, visitors, printed CUI, removable media, printers, destruction, and storage. These responsibilities should remain explicit contractor rows rather than disappearing merely because the MSP does not perform them.

C.10.13 Personnel Security and Training

The contractor normally owns screening, employment status, role authorization, training assignment, and disciplinary processes. The MSP may provide technical access reports and disable accounts, but should not be assigned HR accountability unless a very specific service relationship supports it.

C.10.14 Subcontractors and Other Providers

The contractor or prime must understand what information is flowed down and what systems support performance. The matrix should identify who determines provider requirements, who verifies contractual terms, who tracks current status where required, and who monitors provider changes.

C.10.15 Evidence Repository

Assign who can upload, approve, modify, retain, and retrieve assessment evidence. Evidence should have provenance: date, system, responsible party, requirement relationship, and verification status. A shared folder without ownership rules is not an evidence-management process.

C.11 Responsibility Gaps, Overlaps, and Conflicts

A gap occurs when no party accepts a required activity. An overlap occurs when two parties believe they perform the same activity but do not coordinate. A conflict occurs when documents assign the activity differently. All three can cause assessment and operational failure. The responsibility workshop should therefore search deliberately for blanks, duplicate ownership, and contradictions.

The most dangerous gap is often a handoff gap. HR may notify the contractor manager that an employee departed, but nobody may be responsible for opening the MSP termination ticket. The MSP may be responsible for disabling the account only after receiving the ticket. Each party can truthfully say it performed its assigned task while the former employee retains access. The matrix must map the trigger and the handoff, not only the final technical action.

C.12 The Responsibility Workshop

The responsibility matrix should be built in a working session that includes people who understand contracts, business processes, systems, and provider operations. For a small contractor this may be the owner, security lead, MSP service manager, readiness specialist, and selected technical leads. For a larger organization, include HR, facilities, engineering, legal/contracts, IT, security, and provider representatives as needed.

Work one service or requirement at a time. Describe the real workflow in plain English. Identify the trigger, decision, implementation, recurring operation, evidence, retention, escalation, and independent assessment role. Then compare that description with the SSP, SOW, procedures, tickets, and tool configuration. Do not approve the row until the parties agree that the written assignment reflects reality.

C.13 Translating the Matrix Into the MSA, SOW, and CRM

A responsibility matrix has little value if it contradicts the commercial agreements that govern the provider relationship. After the workshop, assigned provider responsibilities should be reconciled with the MSA, SOW, SLA, service descriptions, and customer responsibility matrix. If the matrix expects a service the provider has not contracted to deliver, either the agreement must change or the matrix must change.

The same rule applies to evidence. If the contractor expects monthly vulnerability reports, annual restore-test evidence, daily alert monitoring, or privileged-access records, the agreement should establish how those records are made available and for how long. Evidence access should not depend on a favor from a technician immediately before an assessment.

						C.14 Sample Detailed Responsibility Matrix

Activity

Contractor

MSP/ESP

Readiness Specialist

Other Provider

C3PAO

Example Evidence

Contract / solicitation review

A/D

C

S

-

-

Contract review record; decision memo

CMMC scope approval

A/D

C/I

S

C

-

Approved scope diagram; inventory; boundary rationale

CUI flow identification

A/D

C

S

C

-

Data-flow diagrams; interviews; process maps

SSP ownership and approval

A/D

C

S

C

-

Approved SSP; revision history

Microsoft government tenant architecture

A/D

I/O

C

I/O

-

Architecture record; tenant configuration; approval

Identity account provisioning

A/D

I/O/E

C

C

-

Approved request; ticket; directory record

MFA / Conditional Access

A/D

I/O/E

C

C

-

Policy export; test evidence; exceptions

Privileged account review

A/D

O/E

C

C

-

Privileged role report; review signoff

Endpoint enrollment / baseline

A/D

I/O/E

C

C

-

MDM/RMM inventory; baseline report

EDR deployment and health

A/D

I/O/E

C

C/O

-

Agent health report; alert records

Patch deployment

A/D

O/E

C

C/O

-

Patch report; exception ticket; validation

Vulnerability scanning

A/D

O/E

C

O/E

-

Scan report; remediation tickets

Firewall rule approval

A/D

I/O/E

C

C

-

Change request; configuration; review

VPN / remote access

A/D

I/O/E

C

C

-

Access approval; VPN config; logs

Backup monitoring

A/D

O/E

C

O/E

-

Job reports; failure tickets

Restore testing

A/D

O/E

C

C/O

-

Restore test record; result; corrective action

Log forwarding

A/D

I/O/E

C

O/E

-

Source list; forwarding config; health alert

SOC alert monitoring

A/D

C/O

C

O/E

-

Alert ticket; escalation record; metrics

Incident technical containment

A/D

O/E

C

C/O

-

Incident ticket; timeline; containment evidence

External incident reporting decision

A/D

C

S/C

C

-

Decision record; report confirmation where applicable

Personnel termination trigger

A/D

O after notice

C

-

-

HR/management notice; service ticket; disable evidence

Physical facility access

A/D/O/E

I

C

-

-

Access roster; visitor logs; reviews

Security awareness training

A/D/O/E

I

C

C

-

Training completion records

Subcontractor flowdown

A/D

I

S

C

-

Subcontract terms; verification records

Evidence repository administration

A/D

O/E

S

C/E

-

Repository permissions; index; retention records

Readiness review

A/D

C/E

S/O/E

C/E

-

Readiness findings; remediation tracker

Level 2 C3PAO assessment when required

A

C/E

C

C/E

ASSESS

Assessment records; evidence requests

Annual affirmation

A/D

C/E

S

C/E

-

SPRS affirmation record; supporting internal approval

Continuous responsibility review

A/D

O/E

S

C/E

-

Quarterly/annual review minutes; updated matrix

Legend: A = accountable; D = decision/approval; I = implementation; O = recurring operation; E = evidence production; S = support/advisory; C = consulted/informed as appropriate; ASSESS = independent assessment role. The legend is deliberately richer than conventional RACI because the operational distinctions matter.

C.15 Sample Responsibility Narrative: Identity and MFA

The contractor determines who is authorized to access the CUI environment and what business role each user requires. HR and management initiate personnel changes. The MSP implements the approved account, assigns the approved groups, enrolls the user in MFA, and applies the defined Conditional Access policies. The contractor security owner approves exceptions. The MSP produces configuration and access evidence. The contractor retains the approved evidence package and remains accountable for ensuring that access decisions are appropriate.

The failure test is straightforward: if an employee leaves at 4:00 p.m., who tells whom, by what method, within what time, who disables each identity, who verifies completion, and what evidence remains? If the matrix cannot answer those questions, the identity responsibility is incomplete.

C.16 Sample Responsibility Narrative: EDR and SOC

The contractor approves the requirement that authorized endpoints be protected and monitored. The MSP deploys the EDR agent and maintains policy configuration. The SOC monitors alerts and escalates according to the agreed severity model. The MSP or SOC may have authority to isolate an endpoint under predefined emergency conditions, while the contractor retains authority over business-impact decisions outside that standing authority. Agent health reports, alert tickets, containment records, and escalation records form the evidence chain.

A missing-agent scenario tests the assignment. The matrix should state who detects that the agent stopped reporting, how quickly the condition is investigated, who reinstalls or repairs the agent, whether the device is restricted while unprotected, who documents the exception, and who verifies closure.

C.17 Sample Responsibility Narrative: Backup and Recovery

The contractor establishes business recovery priorities and approves what data and systems require backup. The MSP or backup provider configures backup jobs, monitors failures, maintains encryption and retention settings, and produces job evidence. Restore testing is separately assigned because backup completion and recoverability are not the same control objective. The contractor reviews test outcomes and accepts remediation where recovery objectives are not met.

A useful matrix does not say merely “Backup - MSP.” It says who decides what is protected, who configures it, who watches it, who responds to failure, who tests restoration, who owns encryption keys if applicable, who retains test records, and who approves changes to retention or architecture.

C.18 Sample Responsibility Narrative: Incident Response

Incident response is a shared workflow with different authorities. The MSP or SOC may be the first party to detect suspicious activity. Technical personnel may collect logs, preserve artifacts, isolate devices, block accounts, and document a timeline. The contractor incident lead coordinates organizational response and determines when legal, contractual, executive, customer, insurer, or government reporting processes are activated. The matrix should identify these decision boundaries before an incident occurs.

The assessment question is not simply whether an incident-response plan exists. The operational question is whether each party knows what happens at 2:00 a.m. when an

alert involves a CUI system. The matrix should be usable during that event without requiring participants to reinterpret the contract under pressure.

C.19 Sample Responsibility Narrative: Microsoft GCC and GCC High

The responsibility matrix should avoid the common mistake of assigning “GCC High compliance” to a single provider. The contractor approves the business and regulatory architecture and determines what data will use the environment. A migration or Microsoft specialist may establish the tenant, domains, identity integration, mail flow, device enrollment, security configuration, and migration. The MSP may then operate users, devices, Exchange, SharePoint, OneDrive, Teams, Defender, and support. The contractor owns decisions about approved use, external sharing, user authorization, and provider oversight.

Evidence responsibility should be equally explicit. Configuration exports, identity reports, device compliance, Defender health, sharing settings, administrative-role reviews, service incidents, and change tickets may come from different portals and providers. The matrix should specify who produces each artifact and where the contractor retains the evidence needed to explain the environment.

C.20 Sample Responsibility Narrative: RMM and Privileged MSP Access

An MSP RMM platform can create a privileged path into many customer systems. The contractor should understand that path even if it does not administer the platform. The MSP should define technician authorization, MFA, privileged-role assignment, session controls, scripting permissions, customer separation, logging, alerting, and termination procedures. The responsibility matrix should also identify who notifies the contractor of material provider-side incidents or architecture changes that could affect the assessed environment.

The strongest test is to select one technician and trace the complete path from employment authorization to RMM login to customer endpoint access. The parties should be able to show approval, authentication controls, role assignment, session evidence where applicable, and removal when access is no longer required.

C.21 Failure Scenarios That Validate the Matrix

C.21.1 Departed Employee Retains Access

HR records the termination, but no ticket reaches the MSP. The matrix should reveal the missing trigger and require verification that all relevant identities, VPN access, cloud sessions, tokens, and physical access are addressed.

C.21.2 EDR Agent Stops Reporting

The SOC sees reduced telemetry, but the MSP assumes the SOC will remediate. The matrix should separate detection, escalation, technical repair, device restriction, and closure evidence.

C.21.3 Firewall Logs Stop Reaching the SIEM

The firewall remains online, the SIEM remains online, but the evidence and monitoring path is broken. The matrix should assign source health, transport health, alerting, remediation, and verification.

C.21.4 Backup Job Is Green but Restore Fails

The backup provider reports successful jobs, but no party owns restore testing. The matrix should make recovery validation a separate responsibility.

C.21.5 CUI Appears in an Unapproved SaaS Tool

A user uploads CUI to a convenience service. The matrix should assign detection, containment, data removal where appropriate, incident evaluation, user follow-up, architecture review, and evidence.

C.21.6 MSP Changes RMM Platform

The MSP improves its service but changes the privileged access architecture. The matrix should define change notification, scope impact review, SSP updates, evidence updates, and validation before assuming the change is neutral.

C.21.7 Provider Incident

A cloud, RMM, SOC, or backup provider experiences a security incident. The matrix should identify notification paths, evidence access, contractor incident evaluation, containment responsibilities, and contractual reporting decisions.

C.22 Responsibility Matrix Change Control

The matrix is a living configuration-management artifact. It should be reviewed when the contractor changes MSPs, adds a provider, adopts a new SaaS platform, changes the CUI boundary, migrates cloud tenants, changes RMM or EDR products, reorganizes personnel, changes facilities, modifies subcontractor relationships, or experiences an incident that exposes an inaccurate responsibility assumption.

Each revision should record the date, reason for change, affected services or requirements, approving parties, related SSP or diagram updates, and any evidence needed to prove the new operating state. A responsibility matrix that is updated only before an assessment will quickly diverge from reality.

C.23 Management Review and Signoff

			Management signoff should confirm more than document receipt. The contractor should confirm that every material

			activity has an accountable owner, provider assignments match contracts, handoffs have triggers and escalation paths, evidence sources are known, independent assessment roles remain independent, and unresolved gaps have an owner and due date. The MSP should confirm that assigned duties match the services it actually delivers and that technicians can perform them using current procedures.

Management Gate

Yes / No / N/A

Owner

Evidence / Notes

Required CMMC level/status and affected systems are understood

Contractor accountability is identified for every material activity

MSP/ESP responsibilities match the SOW/service description

Other-provider responsibilities are documented

Implementation and recurring operation are separately assigned

Evidence producer and evidence owner are identified

Personnel and technical handoffs have defined triggers

Incident authority and escalation are documented

Provider change notification is defined

C3PAO role remains independent where applicable

Matrix agrees with SSP, diagrams, inventories, and provider agreements

Open gaps have owners and target dates

												C.24 Blank Reusable CMMC Responsibility Matrix

Requirement / Activity

Contractor Accountable

Decision / Approval

Implementer

Operator

MSP/ESP

Other Provider

Evidence Producer

Evidence Owner

Frequency

SOW/CRM Ref.

Escalation

Status

								C.25 Provider Responsibility Worksheet

Provider / Service

Data or Security Function

Privileged Access?

Implementation Role

Operational Role

Evidence Supplied

Incident Role

Contract Reference

Change Notification

						C.26 Responsibility Handoff Worksheet

Trigger

Originating Party

Receiving Party

Required Action

Time Expectation

Completion Evidence

Escalation if Missed

Employee termination

New hire / role change

Critical vulnerability

Security alert

Backup failure

Missing EDR agent

Provider incident

Material architecture change

CUI found in unapproved location

C.27 Assessment Interview Preparation Using the Matrix

The matrix can be used to prepare interview participants without scripting artificial answers. Select a requirement or operational activity and ask the accountable contractor representative to explain the process. Then ask the MSP or provider operator to explain the technical execution. Finally, retrieve the evidence identified in the matrix. If the three views disagree, correct the process or documentation before assessment.

This approach also prevents the contractor from sending every technical question to the MSP. The contractor should understand its own system and responsibilities, while the MSP should be prepared to explain the technical services it actually operates. The matrix tells both parties where the boundary lies.

C.28 Technician-Level Use of the Matrix

Technicians do not need to memorize regulatory language to benefit from the matrix. They need to know the approved procedure, the systems they may administer, the evidence their work must leave behind, and when to escalate. A technician-facing view can therefore filter the master matrix to recurring operational rows such as account changes, patching, EDR health, backups, firewall changes, vulnerability remediation, incident handling, and evidence production.

The technician view should never silently redefine accountability. It is an operational extract of the approved master matrix. When a technician discovers that actual

practice differs from the matrix, the correct response is to raise the discrepancy through change control rather than quietly editing the compliance story.

C.29 Executive-Level Use of the Matrix

Executives should use the matrix to answer a different set of questions. Which obligations remain internal? Which functions depend on providers? Which provider failures could interrupt CUI operations or evidence? Are contracts aligned with expectations? Are there responsibilities that only one person understands? Are there material changes that could affect scope or current status? The matrix converts technical complexity into governance visibility.

C.30 Final Responsibility Matrix Standard

A CMMC responsibility matrix is complete only when the contractor and its providers can use it to operate the environment, not merely describe it. Every material responsibility should have an accountable contractor owner, a clear decision authority, an identified implementer and recurring operator, a known evidence producer and evidence owner, a defined escalation path, and an independent assessor role where applicable. Provider assignments should agree with contracts and service descriptions. The matrix should agree with the SSP, diagrams, inventories, procedures, and actual tool configuration.

The final test is operational consistency. Pick a user, endpoint, firewall, backup job, security alert, provider, or CUI workflow and trace responsibility from business decision through technical operation to evidence. Then introduce a failure: a departed user, missing agent, failed restore, lost log source, provider incident, or architecture change. If the parties know who acts, who decides, who records, who escalates, and who verifies closure, the matrix is functioning as intended. If the answer depends on assumptions, the matrix is not finished.

C.31 Current-Requirement Verification Notes

This appendix was written against the CMMC/DFARS framework current in September 2026. Current DFARS 252.204-7021 distinguishes Level 1 (Self), Level 2 (Self), Level 2 (C3PAO), and Level 3 (DIBCAC) requirements and requires applicable contractors to maintain current status, complete annual affirmations, and address flowdown obligations. DFARS 252.204-7025 identifies the CMMC level required by a solicitation and ties award eligibility to current status and affirmation for the applicable contractor information systems. DoD Level 2 scoping guidance also describes ESP considerations and the use of service descriptions and customer

responsibility matrices. Because these requirements can change, readers should verify the current rule, DFARS clauses, solicitation language, and DoD guidance before using this appendix for a specific procurement.

C.32 Deep-Dive: Responsibility Is a Lifecycle, Not a Name in a Cell

A mature responsibility matrix follows a control through its entire life. The lifecycle begins when the organization decides that a safeguard or service is required, continues through design and implementation, becomes an operating process, produces evidence, and eventually changes or retires. This matters because many failures occur after a control has been installed successfully. A firewall can be configured correctly on day one and become ineffective months later because rules accumulate without review. An EDR agent can be deployed to every endpoint and later disappear from a newly imaged laptop. A backup platform can report successful jobs while nobody performs a restoration test. The matrix must therefore describe responsibility over time, not merely responsibility at implementation.

For every significant activity, the contractor should identify the business trigger, the approving authority, the person or provider that performs the technical work, the recurring monitoring or maintenance activity, the evidence created, the person who validates that evidence, the escalation path when something fails, and the event that causes the assignment to be reviewed. This lifecycle view converts the matrix from a compliance spreadsheet into an operating model that can be used by management, technicians, providers, and assessors.

C.33 The Three Layers of Responsibility: Governance, Service Delivery, and Assurance

The first layer is governance. Governance belongs primarily to the organization seeking or maintaining CMMC status. Management determines the business use of CUI, approves scope, selects providers, accepts contractual commitments, approves policy, decides risk treatment, and designates the affirming official. Providers can advise, but the organization must understand and approve the operating model that supports its contractual obligations.

The second layer is service delivery. This is where the MSP, MSSP, ESP, cloud provider, backup provider, identity administrator, or internal IT team performs technical work. Service delivery includes configuration, monitoring, patching, account administration, alert handling, backup operations, log management, and other recurring tasks. A responsibility matrix must be precise enough to distinguish a service the provider merely licenses from a service the provider actively operates.

The third layer is assurance. Assurance asks whether the organization can demonstrate that the designed and operated process is actually occurring. Evidence review, internal validation, management review, readiness activities, self-assessment where applicable, and independent assessment where required all belong here. The C3PAO, when the required status is Level 2 (C3PAO), is an independent assessor rather than an outsourced operator of the contractor's controls.

C.34 Detailed Party Profiles and Interests

C.34.1 Party ABC - Existing Defense Contractor

Party ABC represents an established defense contractor that already performs DoD work and already receives, creates, processes, stores, or transmits information associated with contract performance. Its primary interest is continuity: it must protect the information used in performance while preserving the ability to bid, receive awards, execute work, invoice, collaborate with authorized parties, and maintain the CMMC status required by its contracts. ABC may already have years of technical history, legacy applications, local file shares, remote workers, old firewall rules, unmanaged exceptions, and several third-party providers. Its responsibility exercise therefore begins with discovery and reconciliation. The question is not what a clean-sheet architecture should look like; it is who is actually doing each task today and whether that practice matches the SSP, contracts, service agreements, and evidence.

C.34.2 Party EGH - Prospective DoD Offeror

Party EGH represents a company that wants to enter the defense industrial base or pursue a new category of work. Its interest is readiness before award. EGH has the opportunity to design a smaller, cleaner assessment boundary before CUI is introduced. The responsibility matrix can be used during architecture selection: which employees need access, which cloud environment will be used, which endpoints are authorized, whether an MSP will administer them, how logging and backups will operate, and which provider agreements must be in place. For EGH, responsibility design should occur before procurement and migration decisions become difficult to reverse.

C.34.3 Party IJK - Managed Service Provider / External Service Provider

Party IJK represents the MSP or other external service provider that operates technology for ABC or EGH. IJK's interest is different from the contractor's. It needs a service model that is technically repeatable, contractually clear, supportable by its staff, and capable of producing evidence without creating unlimited or ambiguous

obligations. IJK may operate Microsoft 365, endpoints, firewalls, RMM, EDR, backups, vulnerability tools, ticketing, or monitoring. Its matrix should identify exactly where its responsibility starts and stops, what information or approval it needs from the customer, what service levels apply, what evidence it will retain or provide, and what changes require customer notification or re-scoping.

These party labels are teaching devices, not legal categories. A real organization may combine several roles or use additional specialists. The important principle is to identify interests and authority explicitly so that a provider's technical capability is not mistaken for the contractor's governance responsibility, and the contractor's accountability is not mistaken for an expectation that internal staff must personally perform every technical task.

C.35 Worked Example 1 - Identity, MFA, and Privileged Access

Identity is an ideal example because responsibility crosses business management and technical administration. The contractor determines whether a person should have access. A manager or HR process supplies the authoritative trigger. The MSP may create the account and configure authentication. A security provider may monitor sign-in events. The contractor periodically reviews whether access remains appropriate. Evidence may exist in the identity platform, ticketing system, HR records, and administrative reports. If any one of those handoffs is undefined, a technically correct identity platform can still produce an access-control failure.

Activity	Performer	Accountable/Owner	Typical Evidence
Approve new user and business role	ABC/EGH Management	Contractor	Approval record or onboarding request
Create identity and assign approved groups	IJK MSP	MSP	Ticket + identity audit record
Enroll and enforce MFA	IJK MSP	MSP	Authentication policy/export
Approve privileged role	ABC/EGH Management	Contractor	Privileged-access approval
Assign privileged role	IJK MSP	MSP	Role assignment log
Monitor suspicious sign-ins	SOC/MSP if contracted	Provider	Alert/case record
Periodic access review	ABC/EGH with IJK support	Contractor	Signed access review
Termination trigger	ABC/EGH HR/Manager	Contractor	Termination notice/ticket
Disable account and revoke sessions	IJK MSP	MSP	Ticket + audit log
Verify closure	ABC/EGH designated owner	Contractor	Closure verification

Notice that the MSP can perform most technical actions without becoming the business owner of access. The contractor must provide timely and accurate authorization information. Conversely, the contractor should not claim that it manages MFA merely because management approved the policy if the provider actually configures and monitors the platform. The matrix preserves both truths.

C.36 Worked Example 2 - Endpoint, EDR, Vulnerability, and Patch Chain

Endpoint security is not one responsibility. It is a chain: authorize the device, establish a secure configuration, enroll management tooling, deploy endpoint protection, confirm telemetry, identify vulnerabilities, decide remediation priority, deploy patches or configuration changes, validate success, handle exceptions, and retain evidence. Different products may perform pieces of this chain, but products do not own the workflow.

Lifecycle Step	Primary Performer	Decision/Accountability	Evidence
Authorized-device decision	Contractor	MSP consulted	Approved inventory
Baseline/hardening configuration	Contractor approves	MSP implements	Baseline + configuration evidence
RMM/MDM enrollment	MSP	Contractor informed	Enrollment record
EDR deployment/health	MSP or MSSP	Contractor	Coverage/health report
Alert triage	SOC/MSSP if contracted	Contractor escalation owner	Alert/case record
Vulnerability scanning	MSP/security provider	Contractor	Scan report
Remediation prioritization	Contractor + MSP	Contractor	Remediation decision/ticket
Patch deployment	MSP	Contractor	Patch report/change ticket
Exception/risk approval	Contractor	Contractor	Approved exception
Post-change validation	MSP	Contractor	Rescan/health evidence

C.37 Worked Example 3 - SIEM/SOC and the Evidence Pipeline

A SIEM or SOC relationship is often described too simply as “the provider monitors logs.” A defensible assignment begins at the source. Someone must configure the endpoint, firewall, identity service, server, or cloud platform to generate the required event data. Someone must transport that data. Someone must monitor whether the feed is healthy. The SIEM retains and correlates events. Analysts triage alerts. The customer must have a defined escalation recipient and decision authority. Cases must close with evidence. If the provider receives security protection data on provider assets, the organization must evaluate the ESP relationship and document responsibilities in the SSP and the provider service description/customer responsibility matrix as applicable to the current Level 2 scoping guidance.

Stage	Typical Responsible Party	Evidence
Generate security events	Source system / configured by MSP	Configuration evidence
Forward events	MSP/ESP	Forwarder configuration
Monitor ingestion health	SIEM/SOC or MSP	Health alert/report
Retain/search logs	SIEM provider	Retention configuration
Triage alerts	SOC	Case/ticket
Authorize disruptive containment	Contractor unless pre-authorized	Decision record
Execute technical containment	MSP/SOC per authority	Action log
Close and preserve case evidence	SOC + contractor validation	Case package

C.38 Worked Example 4 - Backup, Restoration, and Business Recovery

Backup responsibilities should be written around recoverability rather than the purchase of a backup product. The contractor identifies the systems and data that matter to business and contract performance, determines acceptable recovery objectives, and approves retention. The provider configures jobs and monitors failures. A separate responsibility must require restoration testing. A green dashboard is evidence that a job ran; it is not by itself evidence that the organization can recover the required information and resume operations.

A complete handoff also covers encryption, administrative access, deletion protection or immutability where used, offsite or alternate storage, failure escalation, restoration authorization, and evidence retention. If the backup provider changes infrastructure or the MSP changes the backup product, the responsibility matrix should trigger an impact review rather than treating the change as an invisible provider implementation detail.

C.39 Worked Example 5 - Incident Response and Reporting Boundaries

Incident response contains both technical and organizational decisions. The SOC may detect an event at 2:00 a.m. The MSP may isolate an endpoint or disable an account if pre-authorized. The contractor determines who has authority to declare an organizational incident, engage leadership or counsel, coordinate contractual reporting, communicate with customers, and approve business-impacting actions. The matrix should distinguish detection, triage, containment, preservation, investigation support, recovery, notification, reporting, lessons learned, and evidence retention.

This distinction is particularly important because a provider cannot safely infer every contractual reporting obligation from a security alert. The provider must know when

and how to escalate; the contractor must know who receives that escalation and who makes the reporting decision. The matrix should reference the incident response plan and the applicable contractual procedures rather than attempting to replace them.

C.40 Worked Example 6 - Microsoft GCC and GCC High Responsibility Model

GCC and GCC High should be treated as service environments with a shared operational model, not as labels that automatically make an organization compliant. A migration or cloud specialist may establish the tenant and move data. Microsoft operates the underlying cloud service within the terms and authorizations applicable to the selected offering. The contractor decides what information and users belong in the environment and approves the architecture. The MSP may administer identities, devices, collaboration settings, security configurations, and support. A security provider may monitor telemetry. The readiness specialist helps map the implemented environment to documentation and evidence. The assessor, when a C3PAO assessment is required, independently evaluates the applicable assessment scope.

The matrix should name responsibilities for tenant ownership, licensing, domain administration, privileged roles, break-glass accounts, MFA, Conditional Access, guest access, external sharing, Exchange, SharePoint, OneDrive, Teams, endpoint integration, Defender services, retention settings, logging, administrative audit records, support cases, incident escalation, configuration changes, and evidence exports. It should also identify who owns the tenant and data if the MSP relationship ends. This exit responsibility is frequently overlooked and should be established before the service begins.

C.41 Software and Licensing Responsibility Register

Technology selection introduces a second form of responsibility: commercial and lifecycle ownership. The party that uses a product is not necessarily the party that owns the subscription, controls the tenant, holds the master administrator account, receives renewal notices, or can export data when the relationship ends. The responsibility matrix should therefore be accompanied by a software and licensing register for every material platform supporting the CMMC environment.

Technology	Commercial/Licensing Owner	Operational Purpose	Responsibility Questions
Microsoft 365 GCC/GCC High	Contractor tenant; reseller/MSP may transact licenses	Identity, collaboration, security configuration	Contractor retains tenant/data ownership and admin recovery path
RMM	Often MSP-owned platform	Remote administration,	MSP must define access,

Technology	Commercial/Licensing Owner	Operational Purpose	Responsibility Questions
		scripting, inventory	logs, customer offboarding/export
EDR/XDR	Contractor or MSP/MSSP subscription	Endpoint detection/response	Define policy ownership, alert operation, evidence access
SIEM/SOC	Provider or contractor platform	Log retention/correlation/monitoring	Define retention, export, escalation, feed health
Backup	Contractor or provider subscription	Backup and restoration	Define retention, encryption, restore testing, exit/export
Vulnerability scanner	Contractor/MSP/provider	Discovery and vulnerability evidence	Define scan scope, credentials, remediation handoff
PSA/Ticketing	Often MSP-owned	Workflow and service evidence	Prevent unapproved CUI; define evidence retention/export
Firewall/VPN management	Contractor appliance; MSP management	Boundary/remote access	Define rule approval, config backup, logs, firmware

The register should include product name, edition, tenant or account identifier, license owner, billing owner, technical administrator, renewal date, data location or service boundary where relevant, evidence export method, support contact, termination procedure, and replacement/transition plan. A product that cannot produce or preserve the evidence the organization needs should be identified as an operational risk before assessment preparation.

C.42 Provider Onboarding and Offboarding

A provider relationship should begin with a controlled onboarding process. The contractor approves the service and the systems the provider may access. The provider identifies named or role-based administrative personnel, authentication requirements, management platforms, remote access paths, data handled, log retention, incident contacts, and evidence that will be supplied. The SSP, network/data-flow diagrams, asset inventory, provider list, and responsibility matrix are then updated together so that the documentation describes the environment that actually exists.

Offboarding is equally important. The matrix should identify who removes provider accounts, revokes tokens and certificates, disables remote-management access, transfers tenant or domain administration, exports logs and tickets, returns or destroys data as required, transfers configuration backups, documents open incidents and

vulnerabilities, and validates that the former provider can no longer reach the environment. The contractor should not discover during a provider dispute that the provider controls the only global administrator account or the only copy of historical security evidence.

C.43 Evidence Ownership, Custody, and Retention

Evidence has an owner even when it is generated by someone else. A SOC may create alert records; an MSP may create change tickets; a cloud platform may create audit logs; a backup provider may create job reports. The contractor should know which evidence it depends on, where it resides, how long it remains available, who can alter or delete it, how it is exported, and how it will be produced during assessment or after a provider change.

For each evidence type, identify the source system, evidence producer, business owner, validation frequency, retention period established by applicable policy or requirement, access restrictions, integrity considerations, export format, repository location, and replacement evidence if the source platform becomes unavailable. Avoid copying uncontrolled screenshots into an evidence folder without provenance. Evidence should be traceable to a system, date, activity, and responsible party.

C.44 Change Events That Must Reopen the Matrix

Change Event	Required Responsibility Review
New contract or solicitation requirement	Review required CMMC status, systems, flowdown, and scope
New CUI workflow	Update data flow, assets, users, providers, controls, and evidence
New MSP/MSSP/ESP	Review provider access, data, service description, CRM, contracts, and scope
Cloud tenant migration	Review identity, data location, integrations, logs, backup, evidence
RMM/EDR/SIEM replacement	Review privileged paths, telemetry, retention, procedures, evidence
Merger/acquisition/network expansion	Evaluate whether assessment scope or architecture materially changes
Office/facility change	Review physical access, networks, media, remote work, diagrams
Major incident	Review failed handoffs, authority, evidence, reporting, corrective actions
Provider ownership/service change	Review contracts, access, data handling, evidence, continuity
Annual affirmation cycle	Confirm assignments still match actual operations and

Change Event	Required Responsibility Review
	documentation

The current Level 2 scoping guidance states that a new assessment is required for significant architectural or boundary changes to the previous assessment scope, while operational changes within the existing boundary that follow the existing SSP may be covered through continuing compliance and annual affirmation. The organization should therefore treat change review as a governance decision supported by current authoritative guidance, not as an informal MSP judgment.

C.45 Assessment-Day Use: Following One Requirement End to End

The strongest way to use the matrix during readiness and assessment preparation is to select one requirement and trace it end to end. Start with the accountable contractor representative. Ask what the organization requires and why. Then ask the implementer to show the configuration. Ask the operator to show how the process is performed repeatedly. Ask the evidence producer to show the resulting records. Finally, verify that the SSP, procedures, diagrams, tickets, reports, and actual system behavior tell the same story. The matrix becomes the index that connects those people and artifacts.

If an answer depends on a provider, the contractor should be able to identify the provider and the exact responsibility rather than responding that “our MSP handles that.” Likewise, the provider should avoid claiming that a tool automatically satisfies a requirement. The useful response explains the configured mechanism, operational process, evidence, and customer/provider boundary.

C.46 Expanded Filled Responsibility Matrix - Example

Activity	Accountable	Decision	Implementer	Operator	Evidence	Frequency/ Trigger
CMMC scope/boundary	Contractor	Contractor	Contractor + MSP input	Contractor	Scope diagram/inventory	On architecture change
CUI data flow	Contractor	Contractor	Contractor + readiness	Contractor	Data-flow diagram	On process change
User authorization	Contractor	Manager/HR	MSP creates account	MSP	Approval + audit log	Each event
MFA/ Conditional Access	Contractor	Contractor policy	MSP	MSP	Policy/export/ report	Continuous + review
Privileged access	Contractor	Contractor	MSP	MSP	Role review/audit	Periodic + event
Endpoint	Contractor	Contractor	MSP	MSP	Baseline/	On change

Activity	Accountable	Decision	Implementer	Operator	Evidence	Frequency/ Trigger
baseline					config report	
EDR coverage	Contractor	Contractor	MSP/MSSP	MSP/MSSP	Health/ coverage report	Continuous
Vulnerability scan	Contractor	Contractor scope	MSP/provider	MSP/provider	Scan report	Defined cadence
Patch remediation	Contractor	Contractor exceptions	MSP	MSP	Patch/change evidence	Defined cadence
Firewall rules	Contractor	Contractor approval	MSP	MSP	Rule/config/ change ticket	On change + review
Log forwarding	Contractor	Contractor	MSP	MSP/SIEM	Forwarder + health	Continuous
SOC alert triage	Contractor	Escalation policy	SOC	SOC	Case/ticket	Continuous
Backup jobs	Contractor	Recovery requirements	MSP/provider	MSP/provider	Job report	Daily/defined
Restore test	Contractor	Contractor	MSP/provider	Contractor validates	Test record	Defined cadence
Incident containment	Contractor	Contractor/ pre-authorized	MSP/SOC	MSP/SOC	Incident record	Per incident
Contractual reporting	Contractor	Authorized official	Contractor	Contractor	Submission/ record	Per event
SSP maintenance	Contractor	Contractor	Readiness + MSP input	Contractor	Versioned SSP	On change/review
Evidence repository	Contractor	Contractor	Contractor/ MSP uploads	Contractor	Indexed evidence	Ongoing
Annual affirmation	Contractor	Affirming official	Contractor	Contractor	SPRS affirmation record	Annual

C.47 Management Signoff Questions Before the Matrix Is Approved

☐ Can management identify every provider that can access CUI or security protection data and explain what that provider does?

☐ Does every material activity have one clearly identified contractor accountability point even when technical work is outsourced?

☐ Do the SSP, diagrams, service descriptions, CRM/SOW/MSA, procedures, and matrix describe the same operating model?

☐ Are implementation and recurring operation separated where different parties perform them?

☐ Are evidence producer, evidence owner, retention location, and retrieval method identified?

☐ Are termination, incident, vulnerability, backup failure, monitoring failure, and provider-change handoffs defined?

☐ Does the contractor retain sufficient tenant, account, data, configuration, and evidence access to transition providers?

☐ Has each provider assignment been confirmed against the service actually purchased rather than assumed capability?

☐ Are changes to scope or architecture routed for CMMC impact review?

☐ Can the organization trace at least one user, endpoint, alert, backup, firewall change, and incident from trigger through evidence?

C.48 Regulatory Verification and 2026 Use Note

This expanded appendix reflects the CMMC and DFARS framework reviewed in September 2026. DFARS 252.204-7021 requires contractors, when the clause applies, to have and maintain the specified current CMMC status for applicable contractor information systems used in contract performance that process, store, or transmit FCI or CUI; it also addresses annual affirmation, reporting in SPRS, and subcontractor requirements. The current DFARS structure distinguishes Level 1 (Self), Level 2 (Self), Level 2 (C3PAO), and Level 3 (DIBCAC). Because contract requirements, implementation phases, guidance, and system architecture can change, readers should verify the solicitation/contract and current authoritative DoD and acquisition sources before using a sample assignment as a final compliance determination.

The current DoD Level 2 Scoping Guide further explains that an ESP may be in scope when CUI or Security Protection Data resides on ESP assets under the stated criteria, and that the ESP relationship and services should be documented in the OSA SSP and described in the ESP service description and customer responsibility matrix. That guidance is one reason this appendix deliberately separates customer and provider duties instead of using the phrase “the MSP handles CMMC.”

Authoritative sources for verification: Defense Federal Acquisition Regulation Supplement (DFARS) 204.75 and 252.204-7021; 32 CFR part 170; and the current DoD CMMC Assessment Scope - Level 2 guidance. These references should be checked again when the book is assembled for publication.

Appendix D
CMMC Technology Stack, Software, Licensing, and Vendor Selection Guide

A Detailed Teaching and Implementation Appendix for MSPs and Defense Contractors

Authored by Dr. Charles Edwards

D.1 Purpose of This Appendix

Technology is necessary to operate a CMMC program, but technology by itself does not create CMMC compliance. A product can provide encryption, identity controls, endpoint telemetry, vulnerability findings, audit logs, workflow, or evidence. The organization still has to decide where FCI and CUI may exist, configure the product correctly, operate it consistently, assign responsibility, preserve evidence, respond to exceptions, and demonstrate that the applicable requirements are actually satisfied.

This appendix therefore teaches technology selection as an architecture and operating-model problem rather than a shopping exercise. It is written for the MSP that must build and maintain customer environments, and for the defense contractor that must understand what it is buying, what remains its responsibility, and what evidence it must be able to produce.

The practical rule carried forward from Appendix C is simple: for every product or service, identify who owns the requirement, who makes the design decision, who implements the technology, who operates it, who reviews the output, who preserves evidence, and who is accountable when the service fails.

D.2 Regulatory Anchor: Start With the Contract and the CMMC Scope

As of this 2026 edition, DFARS 252.204-7021 requires a contractor, when the clause applies, to have and maintain the CMMC status specified by the contracting officer for contractor information systems used to process, store, or transmit FCI or CUI. The clause also addresses annual affirmations of continuous compliance, CMMC UIDs in SPRS, conditional status and POA&M closeout, and flowdown to applicable subcontractors and other contractual instruments.

The technology stack must therefore be derived from the information flow and assessment scope. Buying a product first and trying to make the scope fit the product afterward is the wrong order. The organization should identify the contract requirement, information type, users, endpoints, applications, cloud services, security protection assets, external service providers, and evidence sources before it finalizes the architecture.

The DoD Level 2 Scoping Guide is particularly important to MSPs. It explains that an External Service Provider can be in scope when CUI or Security Protection Data resides on ESP assets, and it calls for the ESP relationship, services, and responsibilities to be documented in the organization's SSP, the ESP service description, and a customer responsibility matrix. This is why software selection and responsibility allocation cannot be separated.

D.3 The CMMC Technology Stack Is a System of Systems

A small defense contractor may begin with the idea that it needs an antivirus product, Microsoft 365, a firewall, and backups. That list is not an architecture. A CMMC-oriented stack must support the complete lifecycle of protected information and the complete lifecycle of security operations: identity creation, access approval, authentication, endpoint configuration, data storage and transfer, network protection, vulnerability discovery, patching, monitoring, alert response, incident handling, recovery, evidence collection, periodic review, and controlled change.

The same product may serve several functions. Microsoft 365 government offerings, for example, can combine collaboration, identity, device management, data protection, audit, and security capabilities depending on licensing and configuration. Conversely, one required capability may be distributed across several products. Vulnerability management may involve a scanner, an RMM platform, endpoint management, ticketing, change control, and an evidence repository.

Capability Layer	Typical Purpose	Evidence Examples
Identity and access	Users, MFA, roles, privileged access, lifecycle	Access reviews, MFA configuration, sign-in logs, admin-role records
Endpoint security	Configuration, EDR, host firewall, encryption	Device inventory, policy status, detections, encryption status
Vulnerability and patching	Discover, prioritize, remediate weaknesses	Scan reports, remediation tickets, patch compliance
Network security	Segmentation, firewalling, VPN,	Rules, diagrams, VPN configuration,

Capability Layer	Typical Purpose	Evidence Examples
	secure connectivity	change records
CUI collaboration	Email, files, sharing, collaboration	Sharing settings, audit records, retention/configuration evidence
Logging/SIEM/SOC	Centralize telemetry and detect events	Log-source inventory, alerts, cases, review records
Backup/recovery	Recover protected systems and information	Job reports, immutable-copy settings, restore tests
RMM/MDM	Operate and configure managed assets	Policy deployment, scripts, inventory, administrative logs
PSA/ticketing	Work tracking and operational evidence	Tickets, approvals, escalation and closure records
GRC/evidence	Map requirements and preserve assessment artifacts	Control records, evidence index, review history

D.4 Microsoft 365: Commercial, GCC, and GCC High Are Not Interchangeable Labels

One of the most common MSP mistakes is to use the words Microsoft 365, GCC, and GCC High as though they describe the same environment with different prices. They do not. Service availability, compliance commitments, identity architecture, endpoints, feature parity, procurement, and data-sovereignty characteristics can differ.

Microsoft states that Microsoft 365 GCC can support FedRAMP High and DFARS-related needs for applicable services, while Microsoft 365 GCC High is positioned for organizations handling DoD CUI and can support CMMC Level 2 and Level 3 requirements when configured appropriately. Microsoft also states that GCC is not suitable for certain CUI Specified categories such as ITAR-controlled information, for which the sovereignty characteristics of GCC High may be necessary. The contractor must determine its actual information and contractual requirements rather than selecting a cloud solely from the phrase 'CMMC compliant.'

D.4.1 What GCC High Changes Operationally

GCC High should be treated as an environment decision, not merely a license upgrade. Microsoft documents separate GCC High endpoints and additional network restrictions. Hybrid identity, migration, external integrations, third-party SaaS connections, mail routing, Teams collaboration, automation, and security tooling

must therefore be validated for the government-cloud environment before the MSP commits to a design.

The MSP should create a government-cloud compatibility register. Every proposed integration should be marked as supported, unsupported, conditionally supported, or awaiting validation. This prevents a commercial-cloud assumption from becoming a production design failure after migration.

D.4.2 Enclave Versus Organization-Wide Government Cloud

An enclave can reduce the number of users, endpoints, and workloads inside the CUI boundary, but it increases the importance of boundary control. The MSP must define how users enter the enclave, how information enters and leaves, what happens to email attachments, whether browser downloads are permitted, how printing and removable media are controlled, how mobile access works, and how accidental CUI spillage into commercial services is detected and handled.

An organization-wide government-cloud deployment can simplify some boundary questions but may increase licensing, migration, and operational costs. The correct design is driven by information flows, business operations, contractual obligations, and the organization's ability to administer the resulting boundary.

D.5 Identity, MFA, and Privileged Access

Identity is the control plane for most modern environments. The MSP should begin with authoritative user sources, joiner-mover-leaver processes, MFA, conditional access, administrative role separation, service accounts, emergency access, and periodic access review. A strong endpoint product cannot compensate for an unmanaged privileged identity.

D.5.1 Licensing Questions

Licensing must be evaluated at the feature level. A tenant may have basic identity licensing but lack the exact conditional-access, privileged-identity, risk, audit, or endpoint capabilities assumed by the design. The bill of materials should therefore identify not only the vendor and SKU but also the security feature being relied upon and the user/device population that requires it.

D.5.2 Evidence Questions

Useful evidence includes identity-provider configuration exports, MFA registration and enforcement records, role assignments, privileged-role activation history where

applicable, access-review records, disabled-account evidence, and tickets showing approval and termination. Screenshots alone are weak when a repeatable export, report, or system record is available.

D.6 Endpoint Management and Endpoint Detection and Response

Endpoint management answers the question 'Is the device configured as required?' EDR answers a different question: 'What is the device doing, and is that behavior malicious or suspicious?' Mature CMMC environments commonly need both configuration enforcement and detection/response capability.

A defensible endpoint design should address inventory, supported operating systems, encryption, screen lock, local administrator control, host firewall, malware protection, EDR health, removable media, software installation, patch state, configuration baselines, and offboarding. The MSP should also define what happens when an endpoint becomes noncompliant: alert only, quarantine, access restriction, ticket creation, or escalation.

D.6.1 EDR/MDR Vendor Selection

Products such as Microsoft Defender and CrowdStrike are examples of platforms that can provide endpoint detection and response capabilities. The book does not designate a universal winner. Selection should consider government-cloud compatibility, data location, telemetry handling, administrative access, incident-retention needs, integration with the SOC, API/export capability, licensing, and the provider's role in the CMMC scope.

If an MDR provider monitors EDR alerts, the responsibility matrix must identify who owns the sensor deployment, who tunes policy, who receives high-severity alerts, who can isolate a device, who communicates with the contractor, who opens the incident record, and who preserves the evidence.

D.7 Vulnerability Management and Patch Management

Vulnerability scanning and patch management are related but not identical. A scanner such as Tenable can identify vulnerabilities and exposure. An RMM, MDM, operating-system update service, or software-management platform may perform remediation. The ticketing system may document ownership and closure. The evidence repository may retain reports needed for assessment.

A strong workflow is: discover assets; scan; validate findings; assign severity and business context; create remediation work; deploy patches or compensating changes; rescan; document exceptions; and periodically report trends. The MSP should avoid claiming that a vulnerability is remediated merely because a patch job was scheduled.

D.7.1 Scanner Licensing

Scanner licensing may be based on assets, IP addresses, agents, cloud workloads, subscriptions, or scanning engines. Before purchase, the MSP should reconcile the licensed quantity with the authoritative asset inventory and expected growth. Under-licensing can create blind spots; over-licensing can unnecessarily increase the customer's recurring cost.

D.8 SIEM, Central Logging, and SOC Operations

A SIEM such as Splunk or Microsoft Sentinel can centralize and analyze security telemetry, but collecting logs is not the same as monitoring them. The operating model must define required log sources, ingestion health, parsing, time synchronization, detection logic, alert ownership, escalation, case management, retention, and periodic review.

For every critical log source, the MSP should document what happens if logs stop arriving. A silent logging failure can undermine both security operations and assessment evidence. The SIEM therefore needs health monitoring as well as threat detection.

D.8.1 Security Protection Data

The MSP must pay special attention to Security Protection Data. Centralized logs, configurations, and security telemetry handled by an ESP can affect CMMC scoping. The service relationship and responsibility allocation should be documented before the customer assumes that outsourcing the SOC automatically places the SOC outside the assessment boundary.

D.9 RMM: Powerful, Necessary, and High-Risk

Remote Monitoring and Management platforms give an MSP extraordinary administrative power. They can inventory devices, run scripts, deploy software, patch systems, open remote sessions, change configuration, and sometimes access sensitive information. That makes the RMM a valuable operations platform and a significant security dependency.

The MSP should protect RMM administrator identities with strong MFA, least privilege, role separation, session logging, restricted technician access, rapid offboarding, approval for high-risk actions, and continuous review. Shared technician accounts should be eliminated wherever the platform supports named accountability.

D.9.1 RMM Evidence

RMM evidence can include device inventory, patch deployment records, script history, remote-session records, configuration status, technician activity, and software inventory. The MSP should know which of these records remain available under the purchased license and for how long.

D.10 PSA and Ticketing Systems

A PSA or ticketing platform often becomes the operational memory of the MSP. It records requests, approvals, incidents, changes, patch exceptions, access provisioning, terminations, vendor escalations, and customer communications. This makes it useful evidence, but it also creates a data-handling risk.

The MSP should establish a rule that technicians do not paste CUI into tickets unless the ticketing environment is explicitly authorized for that information. Ticket attachments, screenshots, exported logs, email-to-ticket ingestion, and AI-assisted ticket features deserve particular scrutiny.

D.10.1 Turning Tickets Into Evidence

A good evidence-producing ticket identifies the system, requester, approver where required, technician, action, date/time, outcome, validation, and closure. For recurring work, templates can standardize the evidence without turning the process into meaningless checkbox activity.

D.11 Secure Email, File Transfer, and Collaboration

CUI moves. It arrives from customers, primes, subcontractors, portals, engineering teams, and government systems. The architecture must therefore control not only where CUI is stored but also how it is exchanged.

Platforms such as Kiteworks and PreVeil illustrate secure collaboration approaches, while Microsoft government-cloud services can provide email and file collaboration capabilities in an appropriately designed environment. Product selection should examine encryption, identity, external sharing, recipient controls, auditability, data

location, administrative access, retention, export, mobile behavior, and integration with the organization's existing identity and endpoint controls.

The central question is not 'Does the product encrypt?' The question is 'Can this organization operate the complete information-sharing workflow in a way that satisfies its applicable requirements and produces evidence?'

D.12 Backup, Recovery, and Resilience

Backups are often treated as an IT utility until an incident occurs. In a CMMC-oriented environment, backup design should identify protected workloads, recovery objectives, backup administrators, encryption, immutability where appropriate, offsite or logically isolated copies, monitoring, failed-job escalation, and restore testing.

A green backup dashboard is not proof of recoverability. The MSP should perform documented restoration tests and retain evidence showing what was restored, from which backup, by whom, how long it took, whether integrity was verified, and what corrective actions resulted.

D.13 Firewalls, VPNs, Segmentation, and Network Security

The network layer enforces boundaries between trusted and untrusted systems and between different internal zones. Firewalls, routers, secure remote access, VPNs, VLANs, DNS security, and network monitoring may all contribute.

For an enclave, the boundary devices deserve special attention because they help establish logical separation. Rules should have business justification, ownership, approval, review dates, and change records. 'Any-any' rules and permanent emergency exceptions should be treated as exceptions requiring documented review rather than as normal operating practice.

D.14 GRC and Evidence Management

GRC platforms such as ServiceNow GRC and specialized CMMC tools can help map requirements, assign owners, track evidence, manage risks, and coordinate remediation. They do not replace the source systems. A GRC record saying that MFA is enabled is weaker than authoritative evidence from the identity system combined with the governance record showing how the requirement is managed.

The evidence repository should preserve provenance. Readers should be able to tell what system produced an artifact, when it was collected, what period it covers, who

reviewed it, what requirement or objective it supports, and whether the artifact contains sensitive information.

D.15 Software Licensing Is Part of the Security Architecture

Licensing is not merely a purchasing issue. Security designs routinely fail because the architecture assumes features that the organization did not buy, did not assign to the right users, or did not enable. Appendix D therefore treats licensing as a configuration dependency.

Product/Service	License Metric	Security Capability Relied Upon	Owner	Renewal/Review
Government collaboration tenant	User/workload/SKU	CUI collaboration, audit, identity integration	Contractor + MSP	Annual and before major scope change
EDR/MDR	Endpoint/user/ workload	Detection, investigation, response	MSP security lead	Monthly utilization; annual renewal
Vulnerability platform	Asset/IP/agent	Scanning and remediation validation	MSP security lead	Quarterly capacity review
SIEM/SOC	Ingestion/data/ retention/service	Central logging and monitoring	Contractor + MSP/SOC	Monthly ingestion and retention review
RMM/MDM	Endpoint/user	Configuration and operational management	MSP operations	Monthly inventory reconciliation
Backup	Workload/storage/ retention	Recovery and resilience	MSP operations	Monthly capacity; annual renewal
GRC/evidence	User/entity/module	Evidence and compliance workflow	Contractor compliance owner	Quarterly access review

D.16 Vendor Due Diligence: Do Not Buy the Marketing Claim

A vendor may say that its product is 'CMMC ready,' 'CMMC compliant,' or 'supports CMMC.' Those statements should trigger questions, not end them. CMMC status belongs to the assessed contractor information system and organization under the applicable framework; a software product does not substitute for the organization's implementation and assessment.

The MSP should request authoritative service descriptions, compliance documentation, architecture information, data-location commitments, subcontractor/subprocessor information where relevant, incident-notification terms, support-access model, encryption details, logging and export capabilities, retention options, government-cloud compatibility, and contract terms.

D.16.1 The Vendor Evaluation Worksheet

Question	Why It Matters	Evidence to Obtain
Where can CUI or security data reside?	Affects scope, data sovereignty, and provider role	Architecture/data-flow documentation
Who can administer or support the service?	Privileged provider access creates risk	Support-access and personnel model
What government-cloud environments are supported?	Commercial integrations may not work in GCC High	Official compatibility statement
Can logs/configurations be exported?	Needed for monitoring and assessment evidence	API/export documentation
What retention is included?	Evidence may disappear before review	Retention schedule and license terms
How are incidents reported?	Customer needs actionable notification	Contract/SLA/incident terms
What is the shared-responsibility model?	Prevents control gaps	CRM/service description
How is the service terminated?	Offboarding must preserve data/evidence	Exit and data-return procedure

D.17 Worked Architecture: Party ABC - Existing Defense Contractor

Party ABC is an established defense contractor that already receives CUI. Its environment grew organically: commercial Microsoft 365, local file shares, an MSP-operated RMM, endpoint antivirus, a firewall, cloud backup, and several engineering applications. The first task is not to replace everything. The first task is to map where CUI and Security Protection Data actually reside and determine which services can remain, which must be reconfigured, which require government-cloud or other compliant alternatives, and which should be removed from the CUI workflow.

ABC's technology project begins with data-flow interviews and technical discovery. The team inventories identities, endpoints, SaaS applications, servers, network segments, remote-access paths, administrative tools, backups, logs, and third-party support. It then marks each component as CUI Asset, Security Protection Asset,

Contractor Risk Managed Asset, Specialized Asset, or out of scope as appropriate to the applicable scoping guidance.

Only after that mapping does ABC select the future stack. If its information requirements drive it toward GCC High, the migration plan must address identity, email, SharePoint/OneDrive, Teams, endpoints, third-party integrations, DNS/network endpoints, archival data, mobile access, and user training. The MSP must also determine which commercial SaaS applications can no longer receive CUI or security data.

D.18 Worked Architecture: Party EGH - Prospective Offeror

Party EGH wants to enter the Defense Industrial Base but does not yet have a mature CUI environment. This gives EGH an advantage: it can design a controlled enclave before CUI begins flowing. The organization can define a limited population of authorized users, managed endpoints, approved collaboration services, secure remote access, centralized logging, EDR, vulnerability scanning, backups, and an evidence repository from the beginning.

The danger is building an enclave that exists only on a diagram. EGH must test real business workflows. Can an estimator receive a controlled drawing? Can engineering collaborate without downloading it to an unmanaged desktop? Can purchasing communicate with a subcontractor? Can an executive review material while traveling? Can support personnel troubleshoot without copying CUI into the PSA? Architecture becomes credible only when those workflows are designed and exercised.

D.19 Worked Architecture: Party IJK - MSP/ESP

Party IJK is the managed service provider. It may operate RMM, EDR, vulnerability management, backup, identity administration, ticketing, SIEM/SOC integration, and user support. Its own systems may therefore hold Security Protection Data and, depending on the service, CUI. IJK cannot assume that being 'the MSP' places its tools outside the customer's assessment concerns.

IJK should maintain a service description and customer responsibility matrix for each standardized service. The CRM should state what the platform does, where customer data and security data reside, what the MSP administers, what the customer must do, what evidence is available, retention, incident escalation, and exit procedures.

Appendix C's responsibility matrix becomes the contract-operational bridge for this work.

D.20 A Practical Technology Selection and Implementation Method

Step 1 - Identify the information and contract requirement

Determine FCI/CUI, CUI categories, export-control or other special handling, required CMMC level/status, and flowdown obligations.

Step 2 - Draw the information flow

Document people, devices, applications, storage, email, collaboration, remote access, providers, backups, logs, and transfer points.

Step 3 - Establish the assessment boundary

Classify assets and providers using the applicable CMMC scoping guidance. Record assumptions and unresolved questions.

Step 4 - Define required capabilities

Translate business workflows and security requirements into identity, endpoint, network, collaboration, monitoring, recovery, and evidence capabilities.

Step 5 - Evaluate products and licenses

Validate government-cloud compatibility, data handling, features, integrations, evidence exports, retention, support model, and cost.

Step 6 - Build the responsibility matrix

Assign ownership, decisions, implementation, operations, evidence, escalation, and review.

Step 7 - Implement and harden

Configure the selected products according to the approved architecture and documented standards.

Step 8 - Validate technically

Test MFA, access, segmentation, logging, alerting, vulnerability detection, patching, backup restoration, and incident workflows.

Step 9 - Collect evidence

Create repeatable evidence procedures rather than one-time screenshots assembled immediately before assessment.

Step 10 - Operate continuously

Review health, alerts, exceptions, access, licenses, integrations, provider changes, and scope changes throughout the contract lifecycle.

D.21 Technology Stack Bill of Materials Template

Category	Selected Product/Service	Edition/SKU	Qty/Metric	Data Handled	Admin Party	Evidence Produced
Identity						
Government collaboration						
Endpoint management						
EDR/MDR						
Vulnerability management						
RMM						
SIEM/SOC						
Firewall/VPN						
Backup/ recovery						
PSA/ticketing						
GRC/evidence						

D.22 Monthly MSP Technology Review

The monthly review converts the architecture into a living operational process. The MSP and contractor should review material changes, not merely whether tools are 'green.' A mature review connects technical health to scope, evidence, responsibility, and business risk.

- Reconcile users, privileged accounts, service accounts, and terminated personnel.
- Reconcile managed endpoints against the authoritative asset inventory.
- Review EDR coverage, unhealthy sensors, high-severity detections, and unresolved cases.
- Review vulnerability trends, overdue remediation, exceptions, and rescan validation.
- Review patch compliance and failed deployments.
- Confirm critical log sources are still reporting to the SIEM/SOC.
- Review backup failures and the status of scheduled restore tests.
- Review firewall/VPN and high-risk administrative changes.
- Review RMM/PSA privileged access and technician changes.
- Check licensing capacity and feature entitlement against the approved architecture.
- Identify new SaaS tools, integrations, subcontractors, or business workflows that may change scope.
- Update the evidence index and responsibility matrix when ownership or technology changes.

D.23 Common Failure Patterns

The most expensive CMMC technology failures are usually not caused by the absence of a famous product. They are caused by gaps between products, people, and responsibility. A customer buys MFA but leaves legacy access paths. It buys EDR but nobody responds to alerts. It buys a scanner but findings never become tickets. It buys a SIEM but key systems stop forwarding logs. It buys backup but never performs a restore test. It moves CUI into a protected enclave but technicians paste controlled screenshots into a commercial PSA.

Another failure pattern is licensing drift. A design assumes a premium security feature, but only some users receive the required license. A renewal changes the SKU. A trial expires. A new acquisition adds endpoints beyond the scanner entitlement. The organization continues to describe the control as implemented even though the technical capability has changed.

The remedy is disciplined architecture management: authoritative inventory, approved standards, responsibility mapping, technical validation, evidence procedures, periodic review, and change control.

D.24 Assessment Preparation: What the Technology Stack Must Be Able to Demonstrate

Before an assessment, the contractor and MSP should be able to demonstrate the environment without improvisation. Administrators should know where authoritative configurations are located, how to generate reports, how to show the scope boundary, how to trace an alert into an incident record, how to demonstrate account lifecycle events, how to show vulnerability remediation, and how to retrieve evidence from prior review periods.

The MSP should not coach personnel to memorize answers. It should make the operating system of the compliance program clear enough that the normal records tell the story. Policies explain what should happen; technology configurations show how the environment is designed; operational records show what actually happened; and interviews connect the two.

D.25 Final Guidance for MSPs and Defense Contractors

The objective of Appendix D is not to produce a universal shopping list. Two organizations can meet the same requirement with different technologies, provided their architecture, implementation, operation, responsibility allocation, and evidence are adequate for the applicable requirements. Product names will change. Licensing will change. Cloud services will change. The disciplined selection method should remain.

For the defense contractor, retain ownership of the compliance decision even when technical work is outsourced. For the MSP, document exactly what the service does and does not do. For both parties, treat every new product, integration, license change, provider, and data flow as a potential architecture and scope change that deserves review.

The most important sentence in this appendix is therefore the simplest: software supplies capabilities; organizations implement and operate requirements.

D.26 Source and Verification Notes for the 2026 Edition

Regulatory statements in this appendix were checked against DFARS 252.204-7021 (NOV 2025), DFARS Subpart 204.75, and current DoD CMMC resources available in September 2026. The Level 2 scoping discussion uses the DoD CMMC

Assessment Scope - Level 2, Version 2.13, including its External Service Provider considerations.

Microsoft government-cloud descriptions were checked against current Microsoft Learn service descriptions and CMMC guidance. Vendor names such as Kiteworks, CrowdStrike, Splunk, Okta, Tenable, ServiceNow, and PreVeil are included as examples of technology categories discussed in the source material that prompted this appendix. Their inclusion is illustrative, not a certification, endorsement, or statement that purchase of a product creates CMMC compliance.

Because product capabilities, licensing, cloud authorizations, and government requirements change, readers should verify current official documentation before procurement or architectural decisions.

D.27 How to Read a Vendor Claim Without Turning It Into a Compliance Conclusion

A security vendor may accurately describe a product as supporting CMMC-related capabilities while the customer still has major implementation gaps. The correct reading of a vendor claim is therefore capability-oriented. Ask what technical function the product provides, what configuration is required, what part of the customer environment it covers, what evidence it can produce, and what responsibilities remain outside the product. This approach prevents procurement language from being mistaken for an assessment result.

The MSP should separate five questions that are often collapsed into one: Is the service technically capable? Is the specific service environment appropriate for the information being handled? Is the customer licensed for the required feature? Has the feature been configured and operated correctly? Can the organization demonstrate the implementation with current evidence? A yes to the first question does not imply a yes to the other four.

This distinction is especially important with cloud platforms. A cloud provider may offer an environment with government-oriented commitments and inherited controls, but the customer remains responsible for customer-side configuration, identities, endpoints, data handling, administrative decisions, monitoring, and many operational activities. The shared-responsibility model must be translated into the customer responsibility matrix described in Appendix C.

D.28 GCC and GCC High: Detailed Decision and Implementation Guide

The GCC versus GCC High decision should begin with information classification and contract analysis, not price. The organization should identify whether it will process ordinary FCI, CUI Basic, CUI Specified, export-controlled information, or other data with special handling requirements. It should then compare those requirements with the official service descriptions and contractual commitments for the proposed cloud environment. Microsoft currently positions GCC High for organizations handling DoD CUI and for requirements such as ITAR, while noting that government-cloud capabilities and feature availability differ by service and configuration.

D.28.1 Phase 1 - Eligibility, Procurement, and Tenant Ownership

Before technical implementation, the contractor should establish who will own the tenant and who will own the commercial relationship. The defense contractor should normally retain durable organizational control over its tenant, domains, data, and emergency administrative access even when an MSP performs day-to-day administration. The MSP can assist with eligibility validation, licensing, and deployment, but the customer should not discover during an MSP transition that the provider alone controls the tenant, DNS, licensing account, or recovery contacts.

The procurement record should identify the legal customer, licensing partner, agreement type, tenant name, verified domains, subscription SKUs, quantity, renewal date, billing owner, technical administrator, security administrator, and escalation contacts. It should also record which security capabilities depend on which licenses. This becomes part of the technology bill of materials and prevents a future renewal from silently removing a control capability.

D.28.2 Phase 2 - Identity and Administrative Design

The first technical design is identity. The implementation team should decide whether identities are cloud-only, synchronized, or federated; how administrators are separated from ordinary user accounts; how MFA is enforced; how emergency access accounts are protected; how service accounts are handled; and how joiner-mover-leaver events are triggered. Privileged administration should be treated as a distinct workflow with approval, strong authentication, named accountability, logging, and periodic review.

An MSP technician should not receive broad tenant privileges merely because the technician works for the provider. Administrative access should be role-based and limited to the services the technician supports. Where delegated administration is used, the provider should document the mechanism, the approved roles, the customer approval process, the logging available, and the procedure for immediate revocation.

D.28.3 Phase 3 - Exchange, SharePoint, OneDrive, and Teams

Collaboration design should define where CUI may be stored and how it may be shared. Exchange rules, SharePoint site permissions, OneDrive sharing, Teams membership, guest access, external federation, anonymous links, synchronization, and mobile access must be reviewed as a single information-flow system. A secure tenant can still produce an insecure workflow if a user can move a protected file into an unauthorized application or share it with an unapproved external identity.

The implementation team should create approved collaboration patterns. For example, a CUI project site can have a defined owner, approved members, controlled guest access, retention settings, sensitivity or handling labels where used, audit logging, and a documented process for adding or removing participants. The purpose is to make the secure workflow easier to follow than an improvised workaround.

D.28.4 Phase 4 - Endpoints and Device Trust

Cloud protection is incomplete if the endpoint that opens the information is unmanaged. The MSP should establish enrollment, encryption, operating-system support, local administrator restrictions, host firewall, malware/EDR protection, screen-lock behavior, patching, removable-media rules, browser controls, and device compliance. Access policies should reflect the organization's risk and architecture so that an unmanaged personal device does not become an accidental extension of the CUI boundary.

D.28.5 Phase 5 - Logging, Monitoring, and Evidence

The team should decide which audit and security records are needed, how long they remain available under the purchased licensing, whether they are exported to a SIEM, who monitors them, and how an assessor or internal reviewer will retrieve them. Evidence procedures should be established during implementation, not weeks before assessment. The same is true for configuration evidence: the organization should know how to show the current state and how to demonstrate that periodic reviews occurred over time.

D.28.6 Phase 6 - Migration and Cutover

Migration is a controlled security change. The plan should inventory source mailboxes, file shares, collaboration sites, archives, local PST files, endpoint caches, and third-party repositories. It should identify the migration tool, temporary storage, administrative credentials, staging systems, rollback method, validation tests, and disposition of the old environment. CUI should not be copied through an unapproved staging service simply because that service is convenient for migration.

Cutover validation should confirm identity, MFA, mail flow, file access, external sharing, endpoint enrollment, security telemetry, backups, logging, and user workflows. The old environment should remain controlled until data disposition and access removal are complete.

D.29 Detailed Endpoint Security Operating Model

Endpoint security should be managed as a lifecycle. The lifecycle begins before a laptop is issued and continues through retirement. Procurement establishes an approved hardware and operating-system baseline. Provisioning applies encryption, management enrollment, EDR, configuration policies, required applications, certificates, and user assignment. Operations maintain patching, sensor health, vulnerability status, and configuration. Offboarding removes access, preserves required evidence, sanitizes or destroys data as appropriate, and updates inventory.

D.29.1 EDR Sensor Health Is a Control Objective

An EDR platform can only observe endpoints on which its sensor is present and functioning. The MSP should therefore monitor coverage as carefully as alerts. A daily or automated health check should identify devices that have not reported, sensors in degraded state, unsupported versions, disabled protection, or endpoints that exist in inventory but not in EDR. Each exception should create a defined response rather than remain an unexplained dashboard count.

D.29.2 Alert-to-Incident Workflow

The workflow should define severity, triage time, escalation path, containment authority, evidence preservation, and closure. If the SOC is permitted to isolate a device immediately, that authority should be documented. If customer approval is required, the escalation path must be fast enough to be operationally meaningful. Closure should record what happened, what was changed, whether credentials were

reset, whether additional endpoints were searched, and whether a broader incident process was triggered.

D.29.3 EDR Licensing and Provider Exit

The license register should record whether the EDR subscription is owned by the customer, resold by the MSP, or bundled into an MDR service. It should also identify what happens to historical telemetry and cases when the subscription ends. The customer should know whether evidence can be exported before termination and whether changing MSPs requires sensor replacement, tenant transfer, or a new security backend.

D.30 Vulnerability Management: From Finding to Verified Closure

A vulnerability report is an input to a process, not the end of the process. The MSP should establish an authoritative asset population, authenticated scanning where appropriate, scan frequency, severity model, remediation time expectations, exception handling, and rescan validation. Findings should be correlated with asset criticality and actual exposure rather than handled only by raw scanner score.

D.30.1 The Seven-State Vulnerability Workflow

State	Meaning	Required Record
Discovered	Scanner or analyst identifies a potential weakness	Finding ID, asset, timestamp, source
Validated	Finding is confirmed or classified	Validation note and owner
Prioritized	Risk and business context are assigned	Severity, due date, rationale
Assigned	Remediation work is given to an owner	Ticket/work item
Remediated	Patch/configuration/mitigation is applied	Change or deployment record
Verified	Rescan or technical test confirms result	Verification evidence
Closed/Excepted	Finding is closed or formally excepted	Closure or approved exception

This workflow prevents the common practice of closing a vulnerability ticket when a patch command was issued rather than when remediation was verified. Exceptions should have an owner, justification, compensating measures where applicable, approval, expiration or review date, and evidence of periodic reconsideration.

D.31 Patch Management: Routine Operations With Assessment Value

Patch management should cover operating systems, third-party applications, browsers, productivity software, server applications, firmware where relevant,

network appliances, and security products. The MSP should define normal maintenance windows, emergency patch procedures, testing expectations, reboot handling, failed deployment escalation, and reporting.

Monthly patch reporting should not hide exceptions inside an overall percentage. A report showing 98 percent compliance can conceal two unpatched internet-facing systems that matter more than dozens of fully patched low-risk endpoints. Reporting should therefore identify critical overdue systems, failed deployments, unsupported software, and approved exceptions.

D.32 SIEM and SOC: Designing the Evidence and Detection Pipeline

A SIEM architecture begins with a log-source inventory. For each source, document what security question the log helps answer, how it is transported, how ingestion health is monitored, what parsing or normalization occurs, how long the data is retained, what detections depend on it, and who owns failures. This creates a defensible reason for collecting each source and a clear response when the source disappears.

D.32.1 Minimum Operational Questions for Every Log Source

- What system generates the record and whose clock is authoritative?
- How is the record transmitted and protected?
- How does the SOC know when ingestion stops?
- Which detections or investigations depend on the source?
- What retention is available under the purchased service?
- Who can search, export, alter, or delete the data?
- What happens to the data if the SOC or SIEM provider changes?

D.32.2 SOC Reporting

The monthly SOC report should summarize material alerts, investigations, confirmed incidents, unresolved cases, log-source health, major detection changes, recurring suspicious behavior, and service exceptions. It should not expose sensitive telemetry to people who do not need it. The report is an operational governance artifact; detailed case evidence can remain in a restricted repository.

D.33 RMM and MSP Privileged Tooling

RMM is one of the most consequential systems in an MSP-operated CMMC environment because it can execute code and administrative actions across many

customer endpoints. The RMM tenant, technician identities, automation scripts, integrations, API keys, and remote-control features should therefore receive security treatment comparable to other privileged infrastructure.

D.33.1 Technician Access Model

Each technician should have a named identity. Roles should distinguish help-desk, endpoint, server, network, security, and administrative functions where the platform permits. MFA should be mandatory. High-risk capabilities such as scripting, mass deployment, credential access, policy changes, and security-tool removal should be restricted and logged. Departed technicians should be removed promptly from the RMM and from every downstream integration.

D.33.2 Script and Automation Governance

Automation improves consistency but can amplify mistakes. Production scripts should have an owner, purpose, version, approval path, test method, and rollback approach. The MSP should distinguish routine approved automation from one-time emergency scripts. Script history can become valuable evidence when it shows when and how a configuration was deployed.

D.34 PSA/Ticketing: Keep Operational Evidence Without Creating a CUI Spill

The PSA should be designed to record the work without becoming an uncontrolled repository for customer protected information. Technicians should be trained to reference secure evidence rather than paste CUI into ticket bodies. Attachments, screenshots, email ingestion, chat transcripts, and AI summarization features should be evaluated because each can create additional storage or processing locations.

A useful ticket template includes customer, system, requestor, approval where required, technician, action performed, validation, evidence reference, exception/escalation, and closure. For access changes, include the identity and role. For security incidents, link to the restricted incident record rather than duplicating sensitive forensic data in a broadly accessible help-desk system.

D.35 Backup and Recovery: Proving That Recovery Works

Backup architecture should define what is protected, frequency, retention, encryption, administrative separation, immutability or deletion protection where appropriate, monitoring, and recovery objectives. The customer and MSP should agree who can

authorize restoration, especially when restoration could overwrite production data or reintroduce compromised content.

D.35.1 Restore-Test Procedure

A restore test should identify the selected workload, backup point, restoration target, technician, start and finish times, integrity checks, application validation, problems encountered, corrective actions, and evidence location. Testing should include representative systems rather than repeatedly restoring the easiest file. A mature program eventually exercises file, application, server, and broader business-recovery scenarios according to the architecture.

D.35.2 Provider Transition

If backup is bundled with the MSP service, the contract should explain what happens at termination. The customer needs a path to retrieve data or transition the service without an unplanned protection gap. Retention after termination, deletion timing, encryption-key ownership, and export feasibility should be known before the relationship ends.

D.36 Secure Collaboration and Controlled External Sharing

External collaboration is where well-designed internal controls frequently fail. The organization should define approved methods for receiving and sending CUI, how recipients are authenticated, whether downloads are permitted, whether links expire, how access is revoked, and how transfers are audited. The approved method should be practical enough that employees do not resort to consumer file-sharing services.

Products such as secure managed file-transfer or encrypted collaboration platforms may fill a specific business need, but the same vendor due-diligence questions apply: where data resides, who can support the service, what identities are used, how encryption and key management work, what audit records exist, how long records remain available, and how the service is offboarded.

D.37 Network Security and Remote Access

Network security should reflect the CUI boundary. The design should identify internet edges, internal segmentation, wireless networks, remote access, administrative paths, cloud connectivity, DNS, and any vendor support tunnels. Diagrams should match actual configurations closely enough that an engineer and an assessor can trace the same path.

D.37.1 Firewall Rule Lifecycle

Every material rule should have a purpose, owner, source, destination, service, approval, implementation date, and review trigger. Temporary rules should expire or be explicitly renewed. Periodic review should identify obsolete objects, broad rules, disabled rules, duplicate rules, stale VPN accounts, and unexpected exposure. The review record becomes both a security artifact and evidence of disciplined operation.

D.37.2 Remote Administration

Remote administration should use approved paths with strong authentication and logging. Direct exposure of management interfaces should be avoided where safer management paths are available. The MSP should document whether technicians connect through VPN, zero-trust access, bastion/jump systems, RMM, or vendor portals, and how each path is revoked during offboarding.

D.38 GRC, Evidence Repository, and Assessment Readiness

The evidence repository should not become a dumping ground. Each artifact should have metadata: requirement or objective supported, source system, collection date, coverage period, collector, reviewer, sensitivity, retention expectation, and replacement schedule. Evidence that expires quickly should be recollected on a defined cadence. Evidence that contains security-sensitive configuration should have restricted access.

A GRC platform can coordinate this process, but the organization should preserve a clear link to authoritative source systems. A manually checked box is not stronger than the technical record it summarizes. The GRC system is most useful when it coordinates ownership, review dates, exceptions, POA&M activity where applicable, and evidence provenance.

D.39 Licensing Deep Dive: Who Owns What and for How Long?

For every recurring security service, the contract and internal register should answer ownership and duration questions. A customer may pay the MSP monthly for a bundled service while the underlying vendor agreement is held by the MSP. That arrangement can be operationally efficient, but it creates transition questions. The customer should know whether the tenant is transferable, whether historical data can be exported, how long the MSP will retain data after termination, and whether a replacement provider can assume administration without rebuilding the service.

Technology	Preferred Ownership Question	Maintenance Responsibility	Exit Question
Microsoft government tenant	Does contractor control tenant/domains and emergency admin?	MSP may administer; contractor governs	Can new MSP assume admin without tenant rebuild?
EDR/MDR	Customer tenant, MSP tenant, or bundled service?	MSP/SOC monitors sensor health and alerts	Can telemetry/cases be exported and sensors transferred?
SIEM/SOC	Who owns workspace and retained logs?	SOC operates; MSP/customer validate sources	How are historical logs/cases preserved?
RMM	Usually MSP platform; customer dependency must be documented	MSP protects platform and technician access	How are agents removed and records exported?
Backup	Who owns vault/account/keys?	MSP monitors jobs and tests restore	How is data transferred or retained at termination?
Vulnerability	Who owns scanner tenant and history?	MSP scans, triages, validates remediation	Can history and exception records be exported?
PSA	Often MSP-owned	MSP protects tickets and access	What customer records/evidence are exported?

D.40 Reporting Framework: Operational, Executive, and Regulatory Records

Reporting should be layered. Technicians need actionable detail; management needs trends, exceptions, and decisions; compliance personnel need traceable evidence; and regulatory or contractual reporting must follow the actual clause and program requirements. Combining all of these into one monthly PDF usually produces a report that serves none of them well.

D.40.1 Monthly Operational Report

- Asset and endpoint reconciliation
- EDR coverage and unresolved high-severity alerts
- Vulnerability findings, overdue remediation, and exceptions
- Patch status and failed deployments
- SIEM log-source health and material SOC cases
- Backup failures and restore-test status
- Privileged-access changes
- Firewall/VPN material changes
- Open security incidents
- Licensing/capacity issues

- New SaaS/providers/integrations
- Evidence collection and scope-change items

D.40.2 Quarterly Management Review

The quarterly review should focus on decisions: unresolved risk, repeated failures, provider performance, budget or licensing constraints, architecture changes, major exceptions, training needs, and upcoming contract or assessment events. Management should approve or assign corrective actions rather than merely receive the report.

D.40.3 Regulatory and Contractual Records

The organization should separately maintain the records needed for its applicable CMMC status, SPRS entries and affirmations, contract flowdown, assessment results, and POA&M closeout where permitted and applicable. The MSP may supply technical evidence, but the contractor should control the business decision and submission process unless an authorized arrangement explicitly states otherwise.

D.41 Expanded Vendor Evaluation Scorecard - Without a Universal Winner

A vendor evaluation should compare facts and requirements rather than declare a universal best product. Weighting depends on the customer architecture. A small enclave may value simplicity and predictable cost; a larger contractor may prioritize API integration, advanced detection, data retention, or multi-tenant administration. The scorecard below is a decision worksheet, not a ranking of vendors.

Evaluation Area	Questions to Ask	Pass/Concern Notes
Information handling	Can the service handle the intended CUI/SPD and contractual constraints?	
Government-cloud compatibility	Does the exact edition/integration support the target environment?	
Identity/MFA	Does it integrate with approved identity and support strong admin authentication?	
Data location/personnel	Where is data stored and who can access/support it?	
Logging/evidence	Can configuration, audit, alerts, and history be exported?	
Retention	Is required operational/evidence history available under the selected license?	

APIs/integration	Do supported APIs work in the government environment?	
Incident terms	How and when is the customer notified?	
Administration	Can least privilege and named technician accountability be enforced?	
Exit/portability	Can data, configuration, and evidence be transferred?	
Cost/licensing	Are all relied-upon security features actually licensed?	
Shared responsibility	Are provider/customer duties documented clearly?	

D.42 Party ABC - Full Technology Modernization Walkthrough

Party ABC begins with an environment that already contains CUI. The first 30 days are discovery and containment of uncertainty. ABC and its MSP inventory data locations, mailboxes, file shares, engineering systems, endpoints, administrators, remote-access tools, backup systems, SaaS applications, and provider relationships. Unknown applications are not automatically declared out of scope; they are investigated until the team can explain whether protected information or Security Protection Data reaches them.

During days 31 through 60, ABC approves the target architecture. The team decides which workloads remain on-premises, which move to the selected government cloud, which SaaS products are prohibited from CUI use, and which security platforms remain. The responsibility matrix is revised at the same time. Procurement and licensing are completed only after feature and environment compatibility are confirmed.

During implementation, identities and administrative roles are cleaned up first, followed by endpoint enrollment, EDR, configuration baselines, collaboration controls, logging, vulnerability management, backup, and network changes. Migration proceeds in controlled waves. Each wave has validation criteria and evidence collection. Users receive workflow-specific training so they know how to handle CUI in the new environment.

The final phase is operational stabilization. ABC reviews sensor health, log ingestion, vulnerabilities, patching, backups, access, incidents, and evidence. The SSP, diagrams, inventory, provider documentation, and responsibility matrix are reconciled against the actual environment. This is the point at which the organization

can credibly say that the architecture described on paper is the architecture being operated.

D.43 Party EGH - Building a CUI Enclave Before the First CUI Arrives

Party EGH can reduce future complexity by refusing to let CUI enter until the approved workflow is ready. It identifies the employees who need access, issues managed devices, creates the protected collaboration environment, establishes identity and MFA, deploys EDR and management, configures secure external sharing, establishes logging and backup, and tests the entire workflow with non-sensitive test data.

The go-live test should simulate actual work: receiving a drawing, saving it, collaborating, sending it to an approved external party, opening it remotely, recovering a deleted copy, terminating a project user, investigating a suspicious login, and producing evidence. Problems discovered during simulation are far cheaper than problems discovered after contract performance begins.

D.44 Party IJK - MSP Standard Service Catalog for CMMC Customers

Party IJK should convert its CMMC-oriented services into a documented service catalog. Each service entry should identify purpose, platform, customer prerequisites, implementation activities, recurring operations, standard reports, evidence available, exclusions, support hours, incident escalation, data handled, retention, licensing model, and termination procedure.

For example, an Endpoint Security Service might include managed EDR, sensor-health monitoring, policy maintenance, alert triage, escalation, monthly reporting, and evidence exports. It should explicitly state whether 24x7 MDR is included, whether the provider can isolate endpoints without customer approval, whether threat hunting is included, how long telemetry is retained, and whether forensic investigation is a separate service. This level of precision prevents the phrase "managed EDR" from hiding different expectations between customer and MSP.

D.45 Ninety-Day Implementation Roadmap

Period	Primary Objective	Key Outputs
Days 1-15	Contract, information, and scope discovery	Data flows, asset/provider inventory, initial

		boundary
Days 16-30	Architecture and gap decisions	Target architecture, responsibility matrix, product decisions
Days 31-45	Procurement and identity foundation	Licenses, tenant ownership, admin model, MFA/access baseline
Days 46-60	Endpoint/network/security deployment	Managed endpoints, EDR, network controls, vulnerability workflow
Days 61-75	Collaboration, logging, backup, integrations	CUI workflows, SIEM/SOC, backup validation, approved integrations
Days 76-85	Evidence and documentation reconciliation	SSP updates, diagrams, evidence index, service descriptions
Days 86-90	Operational validation	Restore test, incident exercise, access review, reporting rehearsal

Ninety days is an illustrative planning framework, not a promise that every organization can reach assessment readiness in ninety days. Existing complexity, contract requirements, migration volume, staffing, procurement lead times, and remediation findings can materially extend the schedule. The value of the roadmap is sequencing: scope before tools, identity before broad deployment, validation before declaration, and operations before assessment.

D.46 Technology Change-Control Triggers

The technology stack should be reopened whenever a change could alter the assessment boundary, information flow, inherited capability, provider relationship, or evidence source. Examples include replacing an MSP, changing RMM or EDR, moving to a new cloud, enabling a new Teams or SaaS integration, acquiring another company, adding a facility, changing identity architecture, introducing AI services, changing backup providers, or moving a security service to an ESP.

Change review should ask four questions: Does the change alter where CUI or Security Protection Data resides? Does it alter who has privileged access? Does it alter how a requirement is implemented or evidenced? Does it alter the documented scope, SSP, diagram, inventory, service description, or responsibility matrix? A yes answer should trigger the appropriate documentation and validation work before the change is considered complete.

D.47 Technology Evidence Catalog

Technology	**Configuration Evidence**	**Operational Evidence**	**Review Evidence**
Identity/MFA	Policies, role configuration,	Sign-in/admin logs,	Access review and privileged-

	authentication settings	provisioning/termination records	role review
Endpoint/EDR	Baseline, EDR policy, encryption settings	Sensor health, detections, isolation actions	Coverage and policy review
Vulnerability	Scan configuration and asset scope	Findings, tickets, rescans	Trend/exception review
Patching	Deployment rings/windows/policy	Deployment results, failures, reboots	Compliance/exception review
SIEM/SOC	Log-source inventory, detection configuration	Alerts, cases, ingestion health	Monthly SOC and source review
Backup	Job, retention, encryption configuration	Job history, failures, restore activity	Restore-test review
Firewall/VPN	Rules, objects, VPN configuration	Change logs, connection/admin logs	Rule and account review
RMM	Roles, MFA, policy, script governance	Technician activity, deployments, sessions	Privileged-access review
Collaboration	Sharing, site, guest, retention configuration	Audit/sharing events	Membership/external-sharing review
PSA	Role and retention configuration	Tickets, approvals, closure	Quality/access review

D.48 Final Detailed Checklist Before a Technology Is Approved

- The business requirement and protected information type are identified.
- The product edition and exact license SKU are documented.
- Government-cloud or target-environment compatibility has been verified from current authoritative documentation.
- Data location, provider access, and third-party/subprocessor considerations have been reviewed.
- The product has an identified owner, administrator, operator, evidence owner, and escalation path.
- Privileged access and MFA requirements are defined.
- Logging, monitoring, retention, and export capabilities are known.
- The integration does not create an unapproved CUI or Security Protection Data path.
- The product is represented correctly in diagrams, inventory, SSP, provider documentation, and responsibility matrix as applicable.
- Implementation and acceptance tests are documented.
- Recurring maintenance and reporting are assigned.
- License renewal and capacity monitoring are assigned.

- Incident-notification and support responsibilities are understood.
- Offboarding, data return, evidence export, and access revocation are documented.
- A scope/change review will occur if the service or architecture materially changes.

D.49 Publication Note: Verify Product Capabilities at Time of Use

This appendix intentionally teaches a durable selection and operating method while naming representative products where doing so helps the reader understand a technology category. Product capabilities, licensing, government-cloud feature parity, endpoints, authorizations, service terms, and vendor ownership can change. Before procurement or implementation, the MSP and contractor should verify the current official service description and contract terms for the exact product edition being purchased.

For the 2026 edition, the Microsoft government-cloud discussion was checked against current Microsoft Learn materials describing GCC, GCC High, government-cloud CMMC support, eligibility, service differences, and GCC High endpoints. The ESP and Security Protection Data discussion was checked against the DoD CMMC Assessment Scope - Level 2, Version 2.13. Regulatory contract language should be checked against the current DFARS clause at the time of contract action or publication.

Appendix E

Sample System Security Plan (SSP) Structure

Detailed Teaching, Documentation, Responsibility, and Evidence Edition

Authored by Dr. Charles Edwards

E.1 Purpose of This Appendix

The System Security Plan is one of the central documents connecting a defense contractor's actual technical environment to its cybersecurity requirements. A useful SSP does more than state that controls exist. It describes the system boundary, operating environment, connections, information flows, responsible parties, and the way required security protections are implemented.

This appendix provides a practical structure that an MSP-supported organization can use when developing or improving an SSP. It is a teaching model, not a mandatory government form. NIST states that there is no prescribed SSP format or specified level of detail, provided the required information is conveyed. The structure presented here is intentionally detailed because MSP-supported environments often distribute implementation and evidence across the contractor, MSP, cloud providers, security platforms, and other External Service Providers.

E.2 Regulatory and Assessment Foundation

For the current CMMC Level 2 context, the SSP should be read together with the applicable contract, DFARS requirements, current CMMC program materials, the Level 2 Assessment Guide, and the security requirements used by the applicable assessment framework. NIST SP 800-171 Revision 2 requirement 3.12.4 requires organizations to develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and relationships with or connections to other systems.

The current CMMC Level 2 Assessment Guide further treats the SSP as an assessable implementation artifact. It identifies system boundary, environment of operation, implementation method, connections and relationships, and a defined update frequency, with at least annual updating identified in the guide. The practical lesson

is that an SSP must describe reality well enough for technical staff and assessors to connect the document to the operating environment.

E.3 The SSP Is Not a Policy Manual

A policy states management expectations. A procedure explains how work is performed. A configuration record shows a technical setting. A ticket shows an operational event. The SSP connects these layers by describing the system and explaining how the organization satisfies its security requirements in that system.

Copying policy language into the SSP without describing implementation creates a document that sounds formal but cannot guide an assessment. Conversely, filling the SSP with raw screenshots and product settings makes it difficult to maintain. The strongest SSP explains the implementation and points to controlled supporting artifacts.

E.4 The SSP Must Describe the Real Environment

The SSP should never describe the environment the organization intends to build someday as though it already exists. Planned safeguards should be clearly distinguished from implemented safeguards. If a deficiency exists, the SSP should accurately describe the current state and the organization's approved remediation mechanism where applicable.

For Party ABC, this means the SSP must describe what ABC actually operates and what Party IJK actually performs. It should not say that ABC performs continuous SIEM monitoring if IJK's SOC performs that work. It should instead explain the service, responsibility, escalation, evidence, and customer oversight.

E.5 SSP Document-Control Page

Field	**Sample Entry / Guidance**
Document Title	System Security Plan - [System/Environment Name]
Organization	Party ABC / Party EGH
System Owner	Name / role
SSP Owner / Custodian	Name / role
Version	Major.Minor
Effective Date	YYYY-MM-DD
Last Review	YYYY-MM-DD

Next Required Review	YYYY-MM-DD or defined trigger
Approval Authority	Name / role
Classification / Handling	Identify appropriate handling; do not overmark
Repository	Controlled document location
Change Record	Reference revision-history section

E.6 Executive System Overview

The opening narrative should allow a knowledgeable manager to understand what the system is, why it exists, what information it handles, who uses it, and how it supports contract performance. It should identify whether the SSP covers the entire enterprise, a CUI enclave, a business unit, a facility, or another defined environment.

Avoid beginning with product names. Begin with the mission and boundary. Products can change while the security purpose remains. A strong overview explains that the environment supports engineering, program management, secure collaboration, or other business functions and then identifies the major technology platforms used to deliver those functions.

E.7 System Identification and Business Purpose

SSP Element	**What to Document**
System Name	Stable name for the assessed environment.
System Identifier	Internal identifier if used.
Business Purpose	Mission/business functions supported.
Contract Context	Applicable contracts/orders/flowdowns without unnecessarily reproducing sensitive content.
Information Types	FCI, CUI categories as applicable, and other relevant information.
User Population	Employees, administrators, subcontractors, remote users, guests where applicable.
Locations	Facilities and remote-work model relevant to the boundary.
Operating Model	Internal, MSP-supported, cloud-centric, enclave, hybrid, or other.

E.8 System Boundary Narrative

The boundary narrative is one of the most important parts of the SSP. It should explain what is inside the environment, what is outside, what connects to it, and why. The narrative should be consistent with the asset inventory, network diagram, data-flow diagrams, provider inventory, and CMMC scoping analysis.

The boundary should not be defined merely by corporate ownership. A contractor may own devices that are out of scope while using an external provider that performs an in-scope security function. The SSP should explain the technical and functional relationships rather than relying on labels.

E.9 Asset Categories and Inventory Relationship

Category / Topic	**SSP Treatment**
CUI Assets	Describe systems/assets that process, store, or transmit CUI and point to inventory.
Security Protection Assets	Describe security functions protecting the assessed environment.
Contractor Risk Managed Assets	Document applicable treatment and organizational management approach.
Specialized Assets	Identify applicable specialized systems and treatment.
Out-of-Scope Assets	Explain separation basis where useful; avoid unsupported declarations.
Inventory Source	Identify authoritative inventory/system of record and reconciliation process.

E.10 Environment of Operation

The SSP should describe the environment in which the system operates: facilities, remote work, cloud services, endpoints, servers, network architecture, administrative model, security operations, backup and recovery, and major external dependencies. This section helps the reader understand how the control implementation descriptions fit together.

For an MSP-supported contractor, include how Party IJK connects, authenticates, administers systems, receives alerts, creates tickets, escalates incidents, and produces evidence. If multiple providers participate, explain the division of functions rather than collapsing them into a generic third-party statement.

E.11 Network and Architecture Diagrams

The SSP should reference controlled diagrams rather than attempt to describe every network relationship in prose. At minimum, the documentation set should make major boundaries, trusted and untrusted connections, cloud services, remote access, security platforms, and relevant data paths understandable.

Diagram	Purpose
High-Level Architecture	Shows major system components, cloud services, facilities, providers.
Network Boundary Diagram	Shows external/internal boundaries and security enforcement points.
CUI Data-Flow Diagram	Shows receipt/creation, processing, storage, transmission, backup, disposition.
Administrative Access Diagram	Shows MSP/admin paths, privileged systems, remote administration.
Logging/Security Telemetry Flow	Shows sources, SIEM/SOC, alert and evidence paths.
Backup/Recovery Flow	Shows protected data, backup service, administrative control, restore path.

E.12 CUI and FCI Data-Flow Narrative

A diagram should be accompanied by a narrative that explains how protected information enters the environment, where it can be stored, who can access it, how it is transmitted, how it is backed up, and how it is ultimately disposed of. The narrative should address normal operations and meaningful exceptions such as secure file transfer, support cases, printing, removable media, or approved external collaboration.

The MSP should specifically examine its own workflows. A ticketing platform, remote support session, log platform, backup service, or technician workstation can become relevant depending on what information is exposed and what function is performed.

E.13 External Connections and Interconnections

Connection	Document
Internet	Boundary protection, permitted services, monitoring.
Remote Users	VPN/ZTNA/other access, authentication, managed-device

	expectations.
MSP Administration	RMM, privileged access, support paths, authorization and logging.
Cloud Services	Service purpose, tenant, information handled, security responsibility.
Subcontractors	Approved information exchange and access path.
Security Providers	SIEM/MDR/backup/vulnerability or other protection services.
Business Partners	Approved exchange method and restrictions.

E.14 External Service Providers and Shared Responsibility

The SSP should identify relevant External Service Providers and describe the service each provides. A service description should answer what the provider does, what systems or information it touches, what security function it performs, what administrative access exists, and what evidence the organization receives.

A responsibility matrix should supplement the SSP. The SSP can summarize responsibility while the matrix provides operational detail. For each major capability, distinguish who owns the requirement, who decides, who implements, who operates, who produces evidence, who maintains the evidence, and who independently assesses when applicable.

E.15 Party ABC / Party IJK Responsibility Example

Capability	**Party ABC**	**Party IJK**	**Evidence**
Identity Governance	Approves users/roles and policy	Administers tenant and lifecycle workflow	Approvals, role reports, sign-in/audit records
Endpoint Security	Defines acceptable use/risk decisions	Deploys and operates endpoint controls	Coverage, policy status, detections
Vulnerability Mgmt	Sets risk priorities/outage decisions	Scans, tickets, remediates within service scope	Scan/rescan, tickets, exceptions
Logging/SIEM	Approves monitoring objectives/escalation	Operates ingestion/alert workflow	Source health, alerts, cases
Backup	Defines business recovery requirements	Operates backup/restore service	Job records, restore tests
Incident Response	Owns organizational/reporting decisions	Detects, investigates, contains as authorized	Timeline, tickets, logs, actions

E.16 Security Requirement Implementation Statement - Standard Pattern

Each implementation statement should answer the same basic questions: what security outcome is required, what technology/process implements it, where it operates, who performs the activity, how often or under what trigger it occurs, what exceptions exist, and what evidence demonstrates operation.

Implementation Element	Question
Scope	Which systems/users/assets does this implementation cover?
Mechanism	What technical or procedural safeguard performs the function?
Configuration	What important settings or rules define the implementation?
Responsibility	Who owns, implements, operates, and reviews it?
Frequency/Trigger	When does the activity occur?
Evidence	What records demonstrate implementation and operation?
Exceptions	What approved limitations or special cases exist?
References	Which policy, procedure, diagram, baseline, or service description supports it?

E.17 Weak Versus Strong Implementation Statements

Weak statement: 'MFA is enabled.' This does not identify scope, exceptions, authentication paths, administration, or evidence.

Stronger statement: 'Party ABC requires multifactor authentication for applicable network and privileged access. Party IJK administers the identity platform under ABC-approved role and access standards. Conditional access and privileged-role configuration enforce the approved authentication paths. Break-glass accounts are restricted, monitored, and reviewed under the emergency-access procedure. Configuration exports, role reports, sign-in logs, and quarterly access-review records provide supporting evidence.'

The stronger statement is still concise, but it tells an assessor and operator where to look and who can explain the implementation.

E.18 Implementation Table Template

Req.	Implementation	Owner / Operator	Evidence /	Status / Notes

	Description		References	
3.x.x	Describe actual implementation in the defined environment.	_____	_____	_____
3.x.x	Describe actual implementation in the defined environment.	_____	_____	_____
3.x.x	Describe actual implementation in the defined environment.	_____	_____	_____

E.19 Access Control Section

The Access Control portion should explain account authorization, role assignment, least privilege, privileged administration, remote access, wireless/mobile access where applicable, session controls, and information-flow restrictions. The SSP should point to identity procedures and configuration evidence rather than reproduce every setting.

In an MSP model, explain how customer authorization reaches the MSP service desk, how technicians obtain administrative privilege, how shared or emergency credentials are controlled, and how customer separation is maintained.

E.20 Awareness and Training Section

Describe who receives security awareness and role-based training, when training occurs, how completion is tracked, and how specialized roles such as administrators or incident responders receive appropriate preparation. If the MSP trains its own technicians separately, distinguish MSP workforce training from the contractor's employee-training responsibility.

E.21 Audit and Accountability Section

Describe what systems generate audit records, where logs are retained, how clocks/time sources are managed where relevant, who reviews security events, how alerting works, and how privileged or sensitive activity is attributable. The SSP should identify dependencies on SIEM, MDR, cloud audit services, or provider portals and explain evidence availability.

E.22 Configuration Management Section

Describe baseline configuration, change approval, secure configuration, least functionality, software control, configuration drift, emergency changes, and how the organization validates that approved changes were successfully implemented. The MSP's RMM, MDM, endpoint management, firewall management, and ticketing processes often provide important implementation and evidence.

E.23 Identification and Authentication Section

Describe unique identification, authentication mechanisms, MFA, password or authenticator management, privileged identities, service accounts, emergency access, and identity lifecycle. The SSP should be clear about identity providers, federated services, and administrative paths.

E.24 Incident Response Section

Describe preparation, detection, triage, escalation, containment authority, reporting decision authority, evidence preservation, recovery, exercises, and lessons learned. The SSP should reference the incident response plan/workflow rather than duplicate it. Where DFARS 252.204-7012 applies, contractual cyber-incident obligations should be addressed in the organization's incident documentation and responsibilities.

E.25 Maintenance Section

Describe authorized maintenance, remote maintenance, maintenance tools, technician authentication, logging, and controls over external maintenance personnel. MSP remote administration should be documented here where it supports maintenance functions.

E.26 Media Protection Section

Describe digital and physical media handling, access, storage, transport, sanitization, destruction, removable media restrictions, and relevant printing processes. If the organization has eliminated certain removable-media workflows, state the enforced design and evidence rather than assuming absence.

E.27 Personnel Security Section

Describe screening and personnel lifecycle security at the level relevant to the system. Explain how termination and transfer events reach system administrators and how access is revoked or changed. The SSP can reference HR procedures while documenting the system-security implementation.

E.28 Physical Protection Section

Describe physical access to facilities and system components, visitor controls, physical access records, and protection of alternate work locations as applicable. Cloud-hosted components should be represented through the service-provider relationship rather than described as though the contractor physically controls the provider's data center.

E.29 Risk Assessment Section

Describe vulnerability scanning, risk assessment, threat and vulnerability information, remediation prioritization, and how findings become corrective actions. Distinguish vulnerability scanning from a broader organizational risk assessment.

E.30 Security Assessment Section

Describe how the organization assesses security requirements, maintains the SSP, tracks corrective actions, reviews control effectiveness, and supports required assessments. The SSP itself should have a defined review/update process and should change when material architecture or responsibility changes occur.

E.31 System and Communications Protection Section

Describe boundary protection, network segmentation, secure communications, cryptographic protections, key management where applicable, remote access architecture, protection of CUI in transit and at rest, and security engineering principles. Reference diagrams and configuration baselines so the narrative remains maintainable.

E.32 System and Information Integrity Section

Describe flaw remediation, malware protection, security alerts/advisories, monitoring for attacks, system/file integrity mechanisms where applicable, and response to

detected weaknesses. Show how EDR, vulnerability management, patching, SIEM, and ticketing work together instead of listing products without workflow.

E.33 Security Requirement Traceability

Requirement	SSP Section	Procedure / Standard	Technology / Service	Evidence Source
3.__.__	E.__	_____	_____	_____
3.__.__	E.__	_____	_____	_____
3.__.__	E.__	_____	_____	_____

Traceability allows the SSP to remain narrative while still giving the readiness team and assessor a direct route from a requirement to implementation and evidence.

E.34 Evidence References Without Turning the SSP Into an Evidence Binder

The SSP should identify evidence sources, but it should not normally embed hundreds of transient screenshots. A better design is to reference an evidence index or repository containing current artifacts. This keeps the SSP maintainable while preserving traceability.

For example, the SSP may state that privileged access is reviewed quarterly and reference the access-review procedure and evidence index. The actual quarterly export, approvals, and remediation tickets remain in the controlled evidence repository.

E.35 Policies, Procedures, Baselines, and Runbooks

Document Type	Role in the Documentation Set
Policy	Management expectation and authority.
SSP	System-specific description of boundary and implementation.
Procedure	Repeatable steps for performing an activity.
Configuration Baseline	Approved technical configuration expectations.
Runbook	Operational instructions for recurring/incident tasks.
Responsibility Matrix	Allocation across contractor/MSP/ESP roles.
Evidence Index	Traceability to current supporting artifacts.
POA&M / Corrective Register	Tracks applicable deficiencies and remediation.

E.36 Planned Controls, Deficiencies, and Honest Documentation

An SSP should not conceal known deficiencies. If a security requirement is not fully implemented, the documentation should accurately represent the current implementation. The organization should then manage remediation through the appropriate internal or formal mechanism. A future-state design can be documented as planned, but it should not be written in present tense as if already operational.

This distinction protects the credibility of the entire assessment package. Contradictions between the SSP, interviews, configurations, tickets, and evidence create more concern than a clearly identified and properly managed deficiency.

E.37 SSP Review and Update Triggers

Trigger	**Required Review**
Annual Review	Formal SSP review/update at the defined cadence.
New CUI Flow	Boundary, data flow, inventory, implementation, providers.
Major Cloud Migration	Architecture, identity, logging, backup, responsibility.
New MSP/ESP	Service description, access, scope, evidence, incident/offboarding.
Security Tool Replacement	Implementation statements, diagrams, evidence sources.
Facility/Network Change	Boundary and physical/network diagrams.
Significant Incident	Affected architecture, lessons, controls, responsibilities.
Acquisition/Merger	Inventory, identities, providers, scope and inherited systems.
Assessment Finding	Implementation description and corrective-action linkage.

E.38 Revision History Template

Version	**Date**	**Author/Owner**	**Change Summary**	**Approved By**
1.0	_____	_____	Initial approved SSP	_____
1.1	_____	_____	_____	_____
2.0	_____	_____	Material architecture/scope revision	_____

E.39 SSP Approval and Governance

The SSP should have an identified owner and approval authority. Approval should mean that management accepts the document as an accurate description of the system and its security implementation, not merely that someone reviewed grammar. Technical owners, the MSP, compliance personnel, and business/system owners may all contribute, but organizational approval should remain clearly assigned.

E.40 SSP Quality Review Checklist

Quality Question	Result
Does the SSP describe the current production environment?	Yes / No / Action
Does the boundary match inventories and diagrams?	Yes / No / Action
Are CUI/FCI flows understandable?	Yes / No / Action
Are MSP/ESP responsibilities accurately described?	Yes / No / Action
Can each requirement be traced to implementation?	Yes / No / Action
Do implementation statements identify actual mechanisms and responsibilities?	Yes / No / Action
Are evidence sources identified and retrievable?	Yes / No / Action
Are deficiencies/planned items represented honestly?	Yes / No / Action
Do policies/procedures/runbooks agree with the SSP?	Yes / No / Action
Is the SSP reviewed at least at the defined cadence and after material changes?	Yes / No / Action

E.41 Party ABC Worked Example - SSP Structure

Party ABC uses a Microsoft government cloud tenant, managed Windows endpoints, a firewall/VPN environment, cloud backup, vulnerability management, and SIEM/MDR services operated in part by Party IJK. ABC's SSP begins with its engineering and program-management mission and identifies the environment in which CUI is created, received, stored, transmitted, and protected.

The SSP does not say simply that 'IJK handles IT.' It identifies IJK's managed services, privileged access paths, ticketing workflow, security platforms, escalation responsibilities, and evidence contributions. ABC remains the organizational owner for scope, contract interpretation, risk decisions, formal representations, and approval of the SSP.

E.42 Party EGH Worked Example - Correcting a Weak SSP

Party EGH begins with an inherited SSP containing generic language copied from a template. It says that the organization reviews logs, performs vulnerability scanning, controls administrative access, and tests backups, but it does not identify the platforms, operators, frequencies, evidence, or exceptions.

During readiness work, EGH and IJK rewrite the implementation descriptions using the standard pattern in this appendix. They discover that several controls are performed by IJK, one backup restore process has never been tested, and an external engineering application is missing from the system diagram. The SSP improvement therefore becomes a technical discovery exercise rather than a writing exercise.

E.43 SSP and Assessment Preparation

Before an assessment, the readiness team should sample SSP statements and attempt to prove them. Select a statement about MFA, logging, vulnerability remediation, backup, or account termination. Ask the responsible person to explain it, retrieve evidence, and demonstrate the mechanism where appropriate. If the statement cannot survive that exercise, the team must determine whether the problem is documentation, evidence, training, or implementation.

This method prevents the SSP from becoming a ceremonial document. It becomes the map used to navigate the real security program.

E.44 SSP Master Outline

Section	Recommended Content
1. Document Control	Title, owner, approval, version, review date.
2. System Overview	Mission, purpose, users, information types.
3. Scope and Boundary	Assets, categories, locations, boundary narrative.
4. Environment of Operation	Architecture, facilities, cloud, endpoints, administration.
5. Information/Data Flows	CUI/FCI lifecycle and approved exchange paths.
6. Connections	External systems, remote access, MSP/ESP integrations.
7. Providers and Responsibilities	Service descriptions and responsibility matrix.
8. Security Requirements	Implementation statements by family/requirement.
9. Supporting Documentation	Policies, procedures, baselines, runbooks, diagrams.
10. Evidence and Traceability	Evidence index/repository references.
11. Deficiencies/Planned Changes	Accurate current state and remediation references.

12. Maintenance and Review	Update cadence, triggers, revision history.
13. Approval	Organizational approval and acknowledgment.

E.45 Closing Perspective

A strong System Security Plan is not strong because it is long. It is strong because it is accurate, maintainable, traceable, and useful. It explains the real system boundary and operating environment, connects requirements to implementation, identifies responsibility, and gives the reader a path to evidence.

For an MSP-supported defense contractor, the SSP is also the place where outsourcing becomes understandable. Party ABC or Party EGH can rely on Party IJK for substantial technical operation without losing visibility into how the environment is protected. When the SSP, responsibility matrix, diagrams, evidence, and operations all tell the same story, assessment readiness becomes much more defensible.

E.46 Deepening the SSP: From Document to Operating Baseline

The SSP becomes substantially more valuable when the organization treats it as an operating baseline rather than a compliance manuscript. Every major statement should be capable of surviving three tests: the responsible person can explain it, the technology or process behaves as described, and current evidence can be retrieved without creating a special artifact solely for the review.

This approach changes SSP maintenance. A change to identity architecture, a new managed security service, a new CUI workflow, or a major network redesign is not merely a technical change. It is also a documentation event. The change process should ask whether the SSP, diagrams, responsibility matrix, procedures, evidence index, and assessment demonstrations require revision.

E.47 The SSP Change-Impact Workflow

Step	Operational Question	Expected Output
1. Identify Change	What system, service, provider, information flow, or responsibility changed?	Change record
2. Test Scope	Does the change affect CUI/FCI handling, security protection, or administrative	Scope impact determination

	access?	
3. Map Requirements	Which implementation statements or assessment objectives may be affected?	Requirement impact list
4. Update Architecture	Do diagrams, inventories, data flows, or connections change?	Updated technical artifacts
5. Update Responsibility	Did owner/operator/evidence duties change?	Updated responsibility matrix
6. Update SSP	Which narrative and implementation statements must change?	Controlled SSP revision
7. Validate Evidence	Can the new state be demonstrated and evidenced?	Acceptance evidence
8. Approve	Who accepts the revised operating state?	Approval/acceptance record

This workflow is particularly important for an MSP because a routine service change can affect many customers. Party IJK should not assume that replacing a security platform is merely an internal tooling decision when the platform performs a customer security function or produces evidence used by the customer's SSP.

E.48 SSP Implementation Statement Worksheet

Field	**Working Entry**
Requirement / Objective	_____
Security Outcome	_____
Assets / Users Covered	_____
Implementation Mechanism	_____
Important Configuration	_____
Customer Decision Owner	_____
MSP / ESP Implementer	_____
Recurring Operator	_____
Evidence Producer	_____
Evidence Custodian	_____
Frequency / Trigger	_____
Exceptions / Limitations	_____
Supporting Procedure / Diagram	_____
Demonstration Method	_____
Last Validated	_____

The worksheet forces the author to resolve ambiguity before writing polished prose. If the team cannot fill in the owner, operator, evidence source, or demonstration method, the problem is probably not a writing problem. It is an implementation or governance problem that should be resolved before the statement is finalized.

E.49 Evidence-to-SSP Traceability Model

Evidence should be traceable in both directions. Starting from the SSP, the reader should be able to find supporting evidence. Starting from an evidence artifact, the team should be able to identify the requirement, implementation statement, system, time period, and responsible activity that the artifact supports.

Evidence Attribute	**Why It Matters**
Evidence ID	Stable reference across reviews and assessment preparation.
Requirement/Objectives	Shows what the artifact is intended to support.
SSP Section	Connects evidence to the documented implementation.
System/Asset	Prevents evidence from the wrong tenant or environment being used.
Period/Date	Shows currency and operating period.
Producer	Identifies the system/person creating the record.
Custodian	Identifies who protects, retains, and retrieves it.
Validation	Records review for completeness and relevance.
Retention	Prevents useful historical evidence from disappearing unexpectedly.

E.50 The SSP and the Customer Responsibility Matrix

For cloud and managed services, the SSP should not attempt to reproduce an entire provider responsibility matrix. Instead, it should explain the service boundary and reference the current responsibility artifact. The team then maps provider responsibilities to the contractor's implementation statements and identifies any responsibility that remains with the customer or MSP.

A common failure occurs when a provider supplies a capability but the customer assumes the provider also performs configuration, monitoring, review, or evidence

retention. The SSP should distinguish inherited or provider-operated capabilities from customer configuration and operational duties.

E.51 Cloud Service Documentation Pattern

Cloud Topic	SSP Questions
Service/Tenant	Which exact service and tenant supports the environment?
Information	What FCI/CUI/security data may be processed, stored, or transmitted?
Identity	How are users/admins authenticated and authorized?
Configuration	Which customer-controlled settings materially affect security?
Logging	What logs exist, who receives them, how long are they retained?
Administration	Who has privileged access and through what path?
Data Protection	How are data at rest/in transit protected within the approved design?
Backup/Recovery	What is provider responsibility versus customer/MSP responsibility?
Incident Interface	How are provider incidents/notices received and escalated?
Evidence	What reports, exports, configurations, or service artifacts support assessment?

E.52 MSP Privileged Access Narrative

The SSP should describe MSP privileged access with enough precision to demonstrate control without publishing unnecessary sensitive details. It should identify the administrative model, named identities or controlled emergency accounts, multifactor authentication, privileged-role assignment, remote-management paths, approval model, logging, session or activity records where available, and periodic review.

Party IJK should be able to show that a technician's ability to administer Party ABC does not imply unrestricted authority. Technical privilege, business authorization, and compliance decision authority are different concepts. The SSP and responsibility matrix should preserve that distinction.

E.53 Service Accounts and Non-Human Identities

Service accounts, API identities, application registrations, automation identities, backup agents, scanners, and integration credentials deserve explicit treatment. They may bypass normal interactive-user workflows while retaining substantial privilege.

The SSP should describe how these identities are approved, scoped, authenticated, protected, rotated where appropriate, monitored, inventoried, and removed. If a legacy service identity cannot support the preferred authentication mechanism, the limitation should be documented and governed rather than hidden inside a generic identity statement.

E.54 Remote Work and Alternate Work Locations

If CUI-related work can occur outside a primary facility, the SSP should explain the approved remote-work architecture. Relevant topics include managed endpoints, remote connectivity, local storage restrictions, printing, physical observation, home networking assumptions, removable media, secure collaboration, and support procedures.

The SSP does not need to describe every employee's home. It does need to describe the organization's controlled operating model and the safeguards that make approved alternate work possible.

E.55 Backup, Recovery, and SSP Accuracy

Backup language should describe more than the existence of a backup product. The SSP should identify what is protected, backup frequency, administrative responsibility, protection of backup data, recovery authority, testing, evidence, and relevant external provider dependencies.

A recurring restore test is especially valuable because it tests both technology and documentation. If a restore exercise reveals that the SSP's stated recovery path no longer matches reality, the documentation should be corrected as part of the same improvement cycle.

E.56 Vulnerability and Patch Management Narrative

The SSP should connect vulnerability discovery to remediation. It should explain scanning or detection coverage, responsible operators, prioritization, ticket creation,

patch or mitigation workflow, exception/risk decisions, rescanning or validation, and evidence.

A statement that the organization 'patches monthly' is rarely enough. Some vulnerabilities require faster action, some systems require maintenance windows, and some findings may need compensating technical action or an approved risk process. The SSP should describe the governing workflow without pretending that every vulnerability follows an identical calendar.

E.57 Logging and Monitoring Narrative

A mature SSP distinguishes log generation, log collection, retention, monitoring, alerting, investigation, escalation, and evidence preservation. These are related but separate activities. A system can generate logs without anyone monitoring them, and a SIEM can collect logs while a critical source is silently disconnected.

The narrative should therefore identify major log sources, monitoring responsibility, source-health checks, alert/case workflow, escalation to the contractor, retention, and evidence. Where Party IJK's SOC performs monitoring, ABC's SSP should explain how ABC retains oversight and receives security-relevant information.

E.58 Incident Reporting Boundary

The SSP should explain the operational incident-response relationship but should not turn every security alert into a contractual conclusion. Party IJK may detect and investigate technical events and provide facts, while Party ABC retains the organizational authority assigned to it for contractual reporting and other external notifications.

The documentation set should identify escalation contacts and decision authority before an incident occurs. The incident response plan then provides the detailed workflow, timelines, preservation steps, communications, and reporting procedures.

E.59 SSP Interview Readiness

Role	Likely SSP Knowledge
Executive/System Owner	Purpose, scope, risk decisions, approval, provider oversight.
Security/Compliance Lead	SSP governance, requirements, evidence, remediation, assessment coordination.
MSP Service Manager	Services provided, responsibility boundaries, escalation, recurring operations.

Identity Administrator	Provisioning, MFA, privileged access, service identities, reviews.
Network/Security Engineer	Boundaries, firewalling, remote access, segmentation, secure communications.
SOC Analyst	Log sources, alerting, investigation, escalation, evidence.
Endpoint Administrator	Baseline, EDR, encryption, patching, configuration management.
Backup Administrator	Coverage, protection, restore process, test evidence.

Interview readiness is not memorization. Personnel should be able to explain the work they actually perform and show where records are produced. If the SSP describes a process that no responsible person recognizes, the documentation and the operating model are misaligned.

E.60 Safe Assessment Demonstration Planning

Technical demonstrations should be planned so that an assessor can observe implementation without creating unnecessary operational risk. The organization should identify appropriate test accounts, non-destructive demonstrations, authorized personnel, expected outcomes, and fallback evidence if a production action would be unsafe.

For example, demonstrating account disablement does not require disabling a production executive account. The team can use an approved test identity or show the workflow and resulting records in a controlled manner. The objective is to demonstrate the mechanism honestly, not to stage an artificial performance.

E.61 SSP Consistency Review Across the Documentation Set

Compare SSP Against	**Consistency Question**
Asset Inventory	Are systems named in the SSP present and categorized consistently?
Network Diagrams	Do boundaries and connections agree?
Data-Flow Diagrams	Do stated CUI paths match the architecture?
Responsibility Matrix	Do owner/operator/evidence roles agree?
Policies	Do management expectations support the implementation?
Procedures/Runbooks	Do operational steps match the SSP narrative?
Tickets/Reports	Does recurring work occur as described?
Evidence Index	Can supporting artifacts be located?
Provider Agreements	Do service commitments support the claimed implementation?

POA&M/Remediation Register	Are known gaps represented consistently?

E.62 Common SSP Failure Modes

The most common SSP failures are not typographical. They are structural: generic template language, obsolete diagrams, product lists without implementation detail, inaccurate claims about provider responsibility, undocumented exceptions, evidence that cannot be retrieved, and future-state controls written as though already implemented.

Another failure is over-detail in the wrong place. Embedding volatile screenshots, IP addresses, individual user lists, or rapidly changing operational data directly in the SSP can make the document stale almost immediately. Stable narrative belongs in the SSP; volatile operational detail belongs in controlled supporting artifacts that the SSP references.

E.63 SSP Review Meeting Agenda

Agenda Item	**Decision / Output**
Scope Changes	Confirm boundary, assets, providers, CUI flows.
Architecture Changes	Confirm diagrams and interconnections.
Responsibility Changes	Confirm customer/MSP/ESP roles.
Implementation Changes	Update affected requirement statements.
Known Deficiencies	Confirm accurate representation and remediation linkage.
Evidence Health	Confirm required evidence is current and retrievable.
Incidents/Lessons	Determine whether controls or narratives changed.
Provider/License Changes	Confirm service capability and responsibility.
Assessment Feedback	Incorporate validated findings.
Approval	Approve revision and next review/trigger.

E.64 Party ABC - Major Cloud Migration Example

Party ABC migrates a CUI-related collaboration workload to a different approved cloud architecture. Party IJK performs the technical migration. The change affects identity, data location, sharing, logging, backup, administration, incident interfaces,

and evidence sources. Treating the project as a simple file migration would leave the SSP inaccurate.

Before operational acceptance, ABC and IJK update the boundary and data-flow diagrams, identify the new provider responsibilities, revise affected implementation statements, test logging and administrative access, verify backup/recovery, and create evidence showing the accepted configuration. ABC then approves the revised SSP because the document now describes the environment that actually entered production.

E.65 Party EGH - MSP Transition Example

Party EGH changes managed service providers. The technical environment initially appears unchanged, but the administrative architecture changes substantially: privileged accounts, RMM tooling, ticketing, monitoring, escalation, backup administration, and evidence custody may all move.

The SSP transition review therefore examines every statement that names or depends on the prior provider. EGH removes obsolete access, establishes Party IJK's approved administrative paths, updates responsibility and evidence ownership, validates security-service health, and records the change before treating the transition as complete.

E.66 Party IJK - Multi-Customer SSP Support Model

Party IJK can improve consistency by maintaining an internal service-to-SSP mapping for each managed security service. The mapping explains the service's technical function, standard operating process, evidence outputs, customer decisions required, and common implementation language. This helps technicians and compliance personnel support multiple customers without copying one customer's facts into another.

The mapping is a starting point, not a universal SSP. Each customer's scope, architecture, contract, configuration, exceptions, and responsibility allocation must still be documented individually.

E.67 SSP Annual Review Certification Worksheet

Review Question	Owner	Result / Evidence

System purpose and boundary remain accurate	_____	_____
CUI/FCI flows remain accurate	_____	_____
Inventories and diagrams reconcile	_____	_____
Provider list and service descriptions are current	_____	_____
Responsibility matrix is current	_____	_____
Implementation statements match operation	_____	_____
Known deficiencies are represented accurately	_____	_____
Evidence sources remain available	_____	_____
Major incidents/changes have been incorporated	_____	_____
Management approval completed	_____	_____

E.68 2026 Publication Note

This appendix is written for the current CMMC Level 2 environment in which Department materials continue to reference the 110 NIST SP 800-171 Revision 2 requirements. NIST withdrew Revision 2 in May 2024 and superseded it with Revision 3; that standards evolution should not be silently substituted for the requirement set specified by the applicable CMMC program materials and contract.

The Department's current Level 2 Assessment Guide states that the SSP should describe the system boundary, environment of operation, implementation of security requirements, and system relationships/connections, and it identifies an update frequency of at least annually. NIST also states that there is no prescribed SSP format or specified level of detail so long as the required information is conveyed. Organizations should verify current official CMMC materials and contractual requirements before assessment or publication.

E.69 Deepened Closing Perspective

The SSP is the narrative backbone of the assessed environment. It should be detailed enough to explain reality, disciplined enough to remain maintainable, and structured enough to connect requirements, people, technology, providers, evidence, and assessment activity.

For an MSP, the central lesson is that documentation quality depends on operational clarity. When Party ABC or Party EGH and Party IJK can answer who owns, decides, implements, operates, produces evidence, maintains evidence, and independently assesses each important function, the SSP becomes easier to write and far more defensible. The document then stops being a static compliance artifact and becomes a reliable map of the security program.

E.70 Building a Complete SSP Package

The SSP should be treated as the central narrative within a controlled documentation package. The narrative explains the system; supporting artifacts prove and operationalize that explanation. A complete package normally includes the SSP, current architecture and data-flow diagrams, asset and provider inventories, responsibility matrices, policies and procedures, configuration baselines, evidence indexes, remediation records, and approval history.

The package should be organized so that a new security manager, MSP service manager, readiness reviewer, or assessor can move from a statement in the SSP to the supporting operational record without relying on tribal knowledge. The objective is not to create more paperwork. It is to make the security program understandable and reproducible.

E.71 SSP Package Index Template

Artifact	Purpose	Owner/Custodian	Review Trigger
System Security Plan	Primary system and implementation narrative	_____	Annual + material change
Boundary/Architecture Diagram	Shows systems, services, boundaries and connections	_____	Architecture change
CUI Data-Flow Diagram	Shows protected information lifecycle	_____	Workflow/service change
Asset Inventory	Authoritative asset population and categorization	_____	Continuous/defined cadence
Provider Inventory	External services and dependencies	_____	Provider/service change
Responsibility Matrix	Allocates owner/operator/evidence duties	_____	Responsibility change
Policies/Procedures	Governance and operational methods	_____	Policy/process change
Configuration Baselines	Approved technical	_____	Platform/baseline change

	expectations		
Evidence Index	Maps implementation to current evidence	_____	Evidence/process change
Remediation Register	Tracks known deficiencies and corrective work	_____	Finding/closure
Revision/Approval History	Shows controlled maintenance and authorization	_____	Every SSP revision

E.72 System Description Worksheet

Topic	**Working Description**
System/Environment Name	_____
Mission/Business Purpose	_____
Contracts/Programs Supported	_____
FCI/CUI Types	_____
Primary User Groups	_____
Facilities/Remote Work	_____
Cloud Services	_____
Endpoints/Servers	_____
Network/Security Services	_____
MSP/ESP Relationships	_____
Primary Administrative Paths	_____
Primary Evidence Repositories	_____

Before writing implementation statements, the team should establish a stable system description. This worksheet captures the facts that should remain consistent throughout the SSP, diagrams, inventories, responsibility matrix, and assessment materials.

E.73 Boundary Validation Workshop

A boundary workshop brings business, technical, MSP, compliance, and provider knowledge together. The group should begin with actual information flows rather than an existing diagram. Follow CUI and FCI from receipt or creation through processing, collaboration, storage, transmission, backup, archival, printing, support, and disposition. Then identify the systems and services that protect those paths.

The workshop should challenge assumptions. If a technician can remotely administer an in-scope endpoint, the administrative path matters. If a ticket can receive screenshots or attachments, the ticketing workflow deserves examination. If security telemetry is sent to an external SOC, the service relationship and evidence path should be documented.

E.74 Boundary Validation Record

Validation Area	Question	Result/Action
Information Flow	Have all normal and exception CUI paths been mapped?	_____
Assets	Do inventories match the boundary narrative?	_____
Security Protection	Are systems/services protecting the environment identified?	_____
Administration	Are internal and MSP privileged paths represented?	_____
Providers	Are relevant ESP/CSP/security services documented?	_____
Connections	Are external/inter-system connections current?	_____
Remote Work	Are alternate-work workflows represented?	_____
Backup	Are backup copies and administration paths represented?	_____
Support/Ticketing	Could protected information enter support workflows?	_____
Evidence	Do evidence systems introduce relevant service dependencies?	_____

E.75 Detailed External Service Provider Record

Every relevant provider should have a concise but complete service record. This prevents the SSP from using vague statements such as 'security is outsourced' or 'Microsoft handles the cloud.' The record should identify the exact service, the function it performs, the information or security data involved, administrative access, responsibility boundaries, incident interface, evidence outputs, and termination requirements.

E.76 Provider Service Record Template

Field	Entry
Provider / Service	_____
Service Purpose	_____
Systems / Assets Involved	_____
Information / Security Data	_____
Security Function	_____
Administrative Access	_____
Customer Responsibilities	_____
Provider Responsibilities	_____
MSP Responsibilities	_____
Logging / Evidence Outputs	_____
Incident Interface	_____
Continuity / Outage Dependency	_____
Offboarding / Data Return	_____
Contract / Service Reference	_____

E.77 Evidence Architecture for the SSP

Evidence architecture is the deliberate design of where assessment-supporting records are created, how they are protected, how long they are retained, and how they are retrieved. Evidence should be a normal output of operations rather than an emergency collection project.

For each major implementation, the team should identify primary evidence, corroborating evidence, and demonstration evidence. Primary evidence directly shows the activity or configuration. Corroborating evidence provides context, such as an approval or ticket. Demonstration evidence shows the mechanism operating under controlled conditions.

E.78 Evidence Mapping Worksheet

Field	Entry
Requirement / Objective	_____
SSP Statement	_____
Primary Evidence	_____

Corroborating Evidence	_____
Demonstration/Test	_____
Producer	_____
Custodian	_____
Repository	_____
Frequency / Freshness	_____
Retention	_____
Last Retrieval Test	_____

E.79 Writing Implementation Statements at Assessment Depth

A substantive implementation statement usually needs more than a product name and a policy reference. It should identify the protected population, mechanism, configuration intent, responsible parties, operating cadence or trigger, exceptions, and evidence. The level of detail should be sufficient for an assessor to understand what to examine, whom to interview, and what could reasonably be tested.

The statement should remain maintainable. Highly volatile values, such as individual account lists or every firewall rule, normally belong in referenced artifacts. The SSP should describe the governing implementation and identify where current details are maintained.

E.80 Access Control - Expanded Sample Implementation

Party ABC authorizes access to the assessed environment based on approved business roles and least-privilege principles. ABC managers approve workforce access and changes in business role. Party IJK administers the identity platform and managed endpoints under ABC-approved procedures. Named administrative identities are used for privileged work where supported, multifactor authentication protects applicable administrative and remote-access paths, and emergency access is restricted and reviewed.

Provisioning begins with an authorized request identifying the user, role, systems, and approving authority. IJK implements approved access and records completion in the service-management system. Termination and transfer events trigger removal or modification of access. Periodic reviews compare active identities and privileged

assignments against current authorization. Evidence includes approved requests, role and group reports, authentication configuration, privileged-role records, sign-in/audit logs, access-review records, and remediation tickets.

E.81 Audit and Accountability - Expanded Sample Implementation

Party ABC and Party IJK maintain audit capabilities across the systems identified in the logging architecture. Relevant endpoints, identity services, cloud platforms, network devices, and security products generate audit or security records. Party IJK operates centralized monitoring services within its assigned scope and maintains defined alert, case, and escalation workflows.

Log-source health is reviewed so that a silent source is not mistaken for an absence of security events. Security alerts are investigated according to severity and service procedures, and material findings are escalated to ABC. Evidence may include log-source inventories, ingestion-health records, retention settings, sample audit records, alerts, investigation cases, escalation tickets, and periodic monitoring reports.

E.82 Configuration Management - Expanded Sample Implementation

ABC establishes approved security and business requirements for the environment. IJK implements and maintains defined secure configurations through endpoint management, RMM, firewall management, cloud administration, and change-control processes. Baselines identify expected settings and permitted functionality, while changes are authorized, tested, documented, and validated according to risk and service impact.

Emergency changes follow an accelerated process but are still documented and reviewed. Drift or configuration exceptions are investigated and either corrected or formally addressed. Evidence includes baseline documents, management-platform policy reports, change tickets, approvals, configuration exports, exception records, and post-change validation.

E.83 Identification and Authentication - Expanded Sample Implementation

ABC uses centrally managed identities for authorized users and administrators. Identity lifecycle activities are tied to approved onboarding, transfer, and termination events. Applicable access paths use multifactor authentication, and privileged roles

are limited to authorized personnel. Service and application identities are inventoried and governed separately from interactive users.

IJK administers identity configuration within its service scope but does not independently decide who should hold a business role. Authentication policies, privileged-role assignments, emergency accounts, service identities, and sign-in activity are reviewed according to defined procedures. Evidence includes identity inventories, MFA and conditional-access configuration, privileged-role reports, service-account records, access-review results, and authentication logs.

E.84 Incident Response - Expanded Sample Implementation

ABC owns organizational incident authority and applicable external reporting decisions. IJK monitors and responds to technical security events within the authority granted by the incident response plan and service agreement. Detection may originate from endpoint, identity, network, cloud, SIEM, user, provider, or service-desk sources.

Events are triaged, classified, documented, and escalated. Authorized containment actions may include endpoint isolation, account disablement, malicious connection blocking, or other defined measures. Evidence preservation and recovery activities are documented. ABC and IJK conduct exercises and use incident lessons to improve controls, procedures, and the SSP. Supporting evidence includes incident tickets, timelines, alerts, logs, containment records, communications, exercise records, after-action reports, and remediation.

E.85 System and Communications Protection - Expanded Sample Implementation

The assessed environment uses defined network and cloud boundaries, controlled remote-access paths, and approved cryptographic mechanisms to protect information in transit and at rest where required by the implementation. Network security devices and cloud controls enforce permitted connectivity, while administrative access follows controlled privileged paths.

ABC approves material architecture and risk decisions. IJK implements and operates assigned network and security services. Diagrams, firewall or security-policy records, VPN or secure-access configuration, encryption status, cloud configuration, change records, and validation tests support the implementation narrative.

E.86 Requirement Implementation Review Rubric

Review Dimension	Strong Condition	Weak Condition
Specificity	Names actual scope/mechanism	Repeats requirement text
Responsibility	Owner/operator clearly separated	Uses vague 'we' or 'IT'
Operation	Explains cadence/trigger/workflow	Describes product existence only
Evidence	Identifies retrievable records	Says evidence exists without source
Exceptions	Known limitations are governed	Exceptions hidden or undocumented
Consistency	Matches diagrams/procedures/configuration	Contradicts supporting artifacts
Maintainability	Stable narrative references volatile detail	Embeds rapidly changing detail
Demonstrability	Personnel can explain/show implementation	Only document author can explain it

E.87 SSP-to-Procedure Alignment Test

Select an SSP statement and locate the procedure that explains how the activity is performed. Then observe or sample an actual record produced by that procedure. If the three disagree, the organization should determine which artifact is wrong. Updating only the SSP may conceal an operational problem; changing only the procedure may leave the SSP inaccurate.

This three-way test - SSP, procedure, evidence - is one of the fastest ways to find documentation drift.

E.88 SSP-to-Technology Alignment Test

Technical validation asks whether the system behaves as the SSP describes. For identity, compare the narrative to actual authentication and privileged-role configuration. For logging, compare the listed sources to SIEM ingestion. For backup, compare the protected-system list to actual jobs and restore evidence. For vulnerability management, compare stated coverage to scanner or management-platform coverage.

Where production testing could create risk, use safe demonstrations, configuration review, controlled test accounts, or other appropriate methods.

E.89 SSP-to-Contract and Service Alignment Test

The SSP should not promise a service that the organization has not purchased or that the MSP is not contracted to perform. Licensing tiers, service descriptions, support agreements, and statements of work should be compared to the security capabilities claimed in the SSP.

This is especially important when a product family has multiple licensing tiers. A security feature appearing in vendor documentation does not prove that the customer's tenant is licensed or configured to use it.

E.90 Technology and License Assurance Record

Field	Entry
Product / Service	_____
Tenant / Subscription	_____
Licensed Tier	_____
Security Capability Relied Upon	_____
Configuration Owner	_____
Operator	_____
Renewal Owner / Date	_____
Evidence of Entitlement	_____
Feature Validation	_____
Fallback / Expiration Impact	_____

E.91 Evidence Freshness and Retrieval Test

An evidence source can exist and still be operationally weak. The readiness team should periodically request a sample artifact without advance preparation. The custodian should retrieve it, explain what it proves, identify its date and system, and connect it to the relevant SSP statement.

Failed retrieval is useful information. It may reveal insufficient retention, unclear custody, weak indexing, provider dependency, or an implementation that is not producing evidence consistently.

E.92 SSP Evidence Sampling Plan

Sample	Implementation	Evidence to Retrieve	Interview/Test	Result
1	Identity / privileged access	Current role/MFA records	Admin interview / safe demo	_____
2	Logging / monitoring	Source health + alert case	SOC interview	_____
3	Vulnerability management	Finding + ticket + rescan	Operator walkthrough	_____
4	Backup / recovery	Job + restore test	Recovery walkthrough	_____
5	Configuration management	Baseline + change record	Configuration review	_____
6	Incident response	Exercise/incident record	Responder interview	_____

E.93 Managing Sensitive Detail in the SSP

The SSP itself may contain sensitive security information. The organization should control access and distribution appropriately. At the same time, the SSP should avoid unnecessary exposure of secrets such as passwords, private keys, recovery codes, or other credentials. Those never belong in the SSP.

Detailed IP addresses, exact detection logic, privileged account names, or other volatile/sensitive values should be included only when necessary and appropriate. Often the better design is to reference a controlled technical artifact.

E.94 Handling Screenshots and Exports

Screenshots can be useful evidence but should be contextualized. A screenshot without tenant, date, system, or explanation can be ambiguous. Whenever practical, preserve native exports, reports, configuration records, or logs alongside screenshots because they may provide stronger traceability and metadata.

Evidence collection should also avoid exposing unrelated customer data. Party IJK must preserve customer separation when exporting reports from shared management platforms.

E.95 SSP Quality Metrics Without Creating a Compliance Score

The organization should not convert SSP quality into a misleading percentage that implies compliance. Operational metrics can instead identify maintenance risk:

number of statements overdue for validation, number of diagrams awaiting update, evidence sources that failed retrieval, unresolved responsibility gaps, or implementation statements affected by recent changes.

These metrics help management prioritize documentation health without pretending that an internal score is an official CMMC result.

E.96 SSP Maintenance Dashboard

Metric	Current	Threshold/Expectation	Action
Statements overdue for validation	___	0 overdue beyond approved cadence	_____
Diagrams awaiting update	___	0 material stale diagrams	_____
Failed evidence retrieval samples	___	Investigate every failure	_____
Open responsibility gaps	___	No unassigned material function	_____
Recent material changes not reflected	___	0	_____
Provider records needing review	___	Current for active relevant providers	_____
Known documentation/implementation conflicts	___	Tracked to closure	_____

E.97 End-to-End Party ABC Case Study - Starting Condition

Party ABC is an established defense contractor supported by Party IJK. ABC has a government cloud collaboration environment, managed Windows endpoints, network security appliances, centralized identity, endpoint security, vulnerability management, backup, ticketing, and SIEM/MDR services. The existing SSP was written before IJK assumed several security operations and before ABC changed its cloud architecture.

The SSP therefore contains accurate high-level policies but stale implementation detail. It names an old remote-management platform, omits a newer security provider, shows an obsolete data-flow diagram, and states that ABC reviews security alerts even though IJK's SOC now performs first-line monitoring.

E.98 Party ABC Case Study - Discovery and Boundary Reconciliation

ABC and IJK begin by reconciling the asset inventory, network diagram, cloud services, CUI workflows, privileged administration paths, security protection services, and external providers. They discover that a support workflow can receive screenshots from CUI systems and that a backup administration portal is accessed by IJK technicians through a privileged management path.

The team does not automatically declare every IJK corporate system in scope. Instead, it documents the actual services, provider assets, security functions, administrative relationships, and information flows relevant to ABC's environment. The resulting boundary narrative is more precise than either 'the MSP is in scope' or 'the MSP is out of scope.'

E.99 Party ABC Case Study - Responsibility Reconciliation

The parties apply the seven-question model to identity, endpoints, vulnerability management, logging, backup, incident response, and change management. ABC retains business authorization, risk acceptance, contract interpretation, scope approval, SSP approval, and formal organizational decisions. IJK implements and operates assigned technical services and produces substantial operational evidence.

They also identify a specialized cloud provider and an MDR platform whose responsibilities must be represented separately. This prevents IJK from being listed as responsible for functions that are actually provider-operated or customer-controlled.

E.100 Party ABC Case Study - Rewriting the SSP

The team rewrites each affected implementation statement using the worksheet in this appendix. Generic language such as 'ABC monitors logs continuously' becomes a precise description of which systems generate logs, which service collects them, which party monitors alerts, how escalation occurs, how source health is checked, and what evidence is retained.

Statements about MFA, vulnerability scanning, backups, incident response, and configuration management are similarly revised. The SSP remains readable because volatile details are moved into referenced inventories, baselines, diagrams, and evidence indexes.

E.101 Party ABC Case Study - Evidence Validation

For each revised statement, the team selects evidence and performs a retrieval test. Identity administrators produce current privileged-role and MFA configuration records. The SOC produces source-health and case records. The vulnerability workflow produces a finding, remediation ticket, and rescan. The backup team produces a restore-test record.

Where evidence cannot be retrieved, the team opens corrective actions rather than marking the statement complete. One recurring report is found to be retained for too short a period to support the organization's intended evidence strategy, so the retention process is revised.

E.102 Party ABC Case Study - Interview and Demonstration Rehearsal

ABC and IJK conduct a structured rehearsal. The system owner explains scope and approval. The identity administrator explains provisioning and privileged access. An IJK SOC analyst explains alert triage and escalation. A technician demonstrates a safe account-management workflow using a test identity. The backup administrator walks through a prior restore test rather than performing a risky production recovery.

The rehearsal reveals terminology inconsistencies between the SSP and technicians' everyday language. The team corrects the documentation and provides role-focused briefing rather than coaching personnel to memorize scripted answers.

E.103 Party ABC Case Study - Operational Acceptance

After the revised SSP, diagrams, responsibility matrix, and evidence mappings are validated, ABC formally approves the new version. Approval records the system owner, document owner, version, date, material changes, and next review trigger. IJK stores its supporting service records and operational procedures in controlled repositories.

The result is not merely a cleaner document. ABC now has a documentation set that matches the operating environment and can be maintained through normal change management.

E.104 Party EGH Case Study - From Template to Real SSP

Party EGH is a smaller contractor whose SSP began as a generic template. Many statements simply repeat requirement language. EGH cannot identify the evidence behind several statements, and responsibility between EGH and its previous provider is unclear.

IJK leads a fact-finding process rather than editing the template sentence by sentence. The team maps CUI workflows, inventories systems, documents providers, identifies technical operators, and tests whether stated safeguards actually exist. Several statements are rewritten, while other areas become remediation items because the claimed implementation is not present.

E.105 Party EGH Case Study - Building Sustainable Maintenance

Because EGH has limited internal staff, the maintenance model assigns clear recurring duties. IJK provides monthly evidence outputs and change notifications. EGH's security lead reviews exceptions, approves organizational decisions, and coordinates SSP updates. A quarterly review examines material changes, evidence health, open remediation, and provider changes.

This model prevents the SSP from becoming dependent on a once-a-year consultant rewrite.

E.106 Party IJK Case Study - MSP SSP Support Factory

Party IJK develops standardized internal service descriptions for identity management, endpoint security, vulnerability management, logging, backup, and incident support. Each description identifies the standard technical function, customer decisions required, operating process, evidence outputs, and common SSP topics affected.

IJK does not provide customers with identical SSP language. Instead, the standardized service records improve accuracy while customer-specific implementation statements reflect each tenant, scope, configuration, contract, and responsibility allocation.

E.107 New Customer SSP Intake Checklist

Intake Area	Required Output
Contract/Requirement Context	Applicable requirement record

Business/System Purpose	System description
CUI/FCI Workflows	Data-flow narrative/diagram
Asset Population	Reconciled inventory
Architecture	Boundary/network diagram
Cloud/Providers	Provider inventory/service records
Administrative Access	Privileged access map
Security Services	Service-to-requirement mapping
Responsibilities	Customer/MSP/ESP matrix
Existing SSP/Policies	Gap/consistency review
Evidence Sources	Initial evidence map
Known Deficiencies	Remediation register
Approval	SSP owner and governance model

E.108 SSP Transition and Offboarding Record

When an MSP relationship ends, the SSP must not continue to describe the former provider as the operator. Offboarding should identify affected implementation statements, administrative paths, evidence custody, service records, integrations, and successor responsibilities.

The departing MSP should provide agreed evidence and transition records, revoke access, and document completion. The contractor or successor provider should validate the new operating state and update the SSP before treating the transition as fully closed.

E.109 Master SSP Authoring Checklist

Checkpoint	**Complete**
Document control and approval fields established	___
Mission and system purpose described	___
Boundary reconciled to inventories and diagrams	___
CUI/FCI flows documented	___
External connections and providers documented	___
MSP/ESP responsibilities mapped	___
Implementation statements describe actual operation	___
All applicable requirement areas trace to evidence	___

Procedures and baselines align with SSP	___
Known deficiencies are represented honestly	___
Evidence retrieval has been sampled	___
Interview and demonstration readiness tested	___
Change/update triggers established	___
Annual review process established	___
Management approval recorded	___

E.110 Substantive Expansion Closing Perspective

The substantive SSP is not a narrative isolated from operations. It is a controlled explanation of the real environment, backed by diagrams, inventories, provider records, responsibility assignments, procedures, technical mechanisms, and evidence.

When maintained this way, the SSP becomes useful long before assessment day. It guides onboarding, change review, incident response, provider oversight, evidence collection, and management decisions. For the MSP, it provides a disciplined way to explain exactly what the provider contributes without absorbing responsibilities that remain with the defense contractor.

E.111 Final Regulatory Verification and Publication Note

This final publication edition was reviewed against authoritative sources available on September 22, 2026. The current CMMC Level 2 Assessment Guide continues to identify CA.L2-3.12.4, System Security Plan, and expects the SSP to describe the system boundary, environment of operation, implementation of security requirements, and connections and relationships to other systems and networks. The guide identifies a defined update frequency of at least annually. It also notes that SSPs often include a general system description, design philosophies, and roles and responsibilities.

NIST SP 800-171 Revision 2 is withdrawn and was superseded by Revision 3 on May 14, 2024. NIST nevertheless states on the Revision 2 publication page that there is no prescribed SSP format or specified level of detail, provided the information required by Requirement 3.12.4 is conveyed. Because CMMC and contractual requirements can specify the applicable baseline, an organization should not silently substitute one NIST revision for another. The solicitation, contract, 32 CFR part 170,

current DFARS clauses, and current Department CMMC materials should be verified for the specific engagement.

The November 2025 version of DFARS 252.204-7021 requires, when the clause applies, a contractor to have and maintain the specified current CMMC status for contractor information systems used in performance that process, store, or transmit FCI or CUI. The clause also addresses annual affirmation of continuous compliance, CMMC unique identifiers in SPRS, applicable flowdown, and closeout of a valid POA&M when Conditional status applies. These obligations reinforce the need for the SSP to describe the actual contractor information systems and provider relationships used in contract performance.

E.112 Final SSP Publication Standard

Publication Standard	**Final Requirement**
Accuracy	The SSP describes the current operating environment, not an aspirational future state.
Boundary	System boundary, CUI/FCI flows, relevant security protection, and connections are understandable and reconcile with diagrams and inventories.
Implementation	Security requirement statements explain actual mechanisms, responsibilities, cadence/triggers, exceptions, and supporting artifacts.
Responsibility	Contractor, MSP/MSSP/ESP, cloud/provider, readiness, and independent assessment roles are not blurred.
Evidence	Statements point to retrievable operational evidence without turning the SSP into a screenshot repository.
Provider Relationships	Relevant external services are documented with service boundaries and customer/provider responsibility.
Consistency	SSP, responsibility matrix, diagrams, policies, procedures, tickets, configurations, and evidence tell the same story.
Maintenance	The SSP has an owner, approval authority, revision history, at-least-annual review, and material-change triggers.
Assessment Readiness	Responsible personnel can explain the implementation and safely demonstrate or substantiate it.
Authority	The SSP does not replace the applicable contract, regulation, official assessment guide, or authoritative NIST publication.

E.113 Final Terminology and Responsibility Consistency

Throughout this appendix, 'owner' means the party or role accountable for a decision or organizational outcome; 'operator' means the party performing recurring technical or procedural work; 'evidence producer' means the system, process, or person that creates the record; and 'evidence custodian' means the party responsible for controlled retention and retrieval. These roles may be assigned to different organizations.

Party ABC and Party EGH represent defense-contractor customers. Party IJK represents an MSP, MSSP, or other external service provider depending on the example. Party IJK can implement and operate substantial security capabilities and can produce assessment-supporting evidence, but technical operation does not automatically transfer the contractor's organizational accountability, contract interpretation, scope approval, formal affirmation, or other decisions reserved to the contractor.

A readiness or compliance specialist supports preparation, interpretation, documentation, gap identification, and evidence organization. A C3PAO, when applicable, performs an independent assessment role. Preparation and independent assessment should remain conceptually distinct.

E.114 Authoritative Sources Used for Final Verification

The final verification used the current Department of Defense CMMC Level 2 Assessment Guide for CA.L2-3.12.4; NIST SP 800-171 Revision 2 and its publication status; NIST SP 800-171 Revision 3; DFARS 252.204-7021 (NOV 2025); DFARS subpart 204.75; and the applicable framework in 32 CFR part 170. Readers should verify the current versions of these authorities when using the appendix for a live solicitation, contract, assessment, or formal compliance decision.

This appendix is an educational and operational structure. It does not create a mandatory SSP template, determine assessment scope by itself, or substitute for legal, contracting, assessment, or organization-specific professional judgment.

E.115 Final Publication Closing Perspective

The final purpose of an SSP is not to impress the reader with volume. Its purpose is to make the protected environment understandable and defensible. A strong SSP tells a consistent story about the system boundary, information flows, technology, people, providers, responsibilities, security implementation, and evidence.

For MSP-supported defense contractors, that consistency is especially important because responsibility is distributed. The contractor must understand what it owns and approves; the MSP must understand what it implements and operates; providers must be represented accurately; evidence must remain attributable and retrievable; and independent assessment must remain independent. When those relationships are explicit, the SSP becomes both an assessment artifact and a practical operating map.

Appendix E is therefore intended to be used alongside the readiness checklist, scoping checklist, responsibility matrix, technology and licensing guide, POA&M structure, assessment preparation checklist, technician checklist, onboarding/offboarding workflow, incident response workflow, CMMC/NIST cross-reference, glossary, and continuous-readiness toolkit contained in the remaining appendices of this book.

Appendix F
Sample Plan of Action and Milestones (POA&M) Structure

Detailed Teaching, Remediation, Tracking, and Closeout Edition

Authored by Dr. Charles Edwards

F.1 Purpose of This Appendix

A Plan of Action and Milestones is not merely a spreadsheet containing weaknesses and due dates. Used correctly, it is a controlled management record that explains what remains to be corrected, why the deficiency matters, who owns the correction, what resources and dependencies are required, how progress will be measured, and what objective evidence will prove that remediation is complete. For an MSP, the POA&M also creates a disciplined bridge between technical work, customer management, compliance personnel, and assessment preparation.

This appendix makes an important distinction from the beginning. Organizations may use internal remediation plans for ordinary cybersecurity weaknesses, audit findings, technical debt, or improvement projects. A formal CMMC assessment POA&M, however, is governed by the CMMC rules and is not available for every level or every unmet requirement. The existence of an internal POA&M must never be presented as proof that an organization is entitled to Conditional CMMC Status.

F.2 Current CMMC POA&M Rules — The Boundary the Reader Must Understand

As of the 2026 edition of this book, CMMC permits only limited use of assessment POA&Ms. DoD's current CMMC program information states that Level 1 does not permit POA&Ms. Level 2 may permit a POA&M under the conditions in 32 CFR 170.21, and a valid POA&M supporting Conditional Level 2 status must be closed within 180 days. DFARS 252.204-7021 likewise defines a current Conditional Level 2 status as not older than 180 days and requires a contractor with Conditional status to successfully close out a valid POA&M to achieve Final status.

This means a contractor should never use the sentence, “We can just put that on a POA&M,” as a substitute for understanding the applicable rule. The assessment team must determine whether the unmet objective is eligible, whether the required

minimum conditions for Conditional status are met, and whether the item is prohibited from POA&M treatment under the governing CMMC rule. This appendix teaches the management structure; the organization must verify current eligibility rules against 32 CFR part 170 and current DoD guidance at the time of assessment.

F.3 Internal Remediation Plan Versus CMMC Assessment POA&M

An internal remediation plan is a management tool. A company can use one whenever it discovers a weakness: an EDR agent that stopped reporting, a firewall rule that is too broad, an overdue access review, an unsupported workstation, a failed backup restoration, or a documentation inconsistency. Internal remediation should begin as soon as the problem is discovered.

A CMMC assessment POA&M is different. It exists in the context of an assessment result and Conditional CMMC Status. It is constrained by the CMMC program. The contractor should therefore maintain two concepts in its governance model: continuous internal remediation, which should be routine, and formal CMMC post-assessment remediation, which is a regulated path with specific eligibility and closeout requirements.

F.4 What a High-Quality POA&M Record Must Explain

A useful POA&M record tells a complete story. A manager who was not present when the weakness was discovered should be able to understand the affected requirement, system, business process, technical condition, risk, root cause, corrective strategy, responsible party, milestones, dependencies, target date, validation method, evidence location, and final closure decision.

The description should be specific enough to act upon. “Fix MFA” is not a remediation plan. A stronger record might explain that three legacy service accounts are exempt from the organization's normal MFA policy, identify the applications that depend on those accounts, describe the replacement authentication design, assign application owners and MSP engineers, establish test and cutover milestones, and define the evidence required to demonstrate that the legacy path has been removed.

F.5 Core POA&M Data Fields

Field	What It Should Capture	Why It Matters
POA&M ID	Unique identifier	Allows traceability across tickets, evidence, assessment records, and reports.
Requirement / objective	Applicable requirement and assessment	Connects remediation to the condition being

Field	What It Should Capture	Why It Matters
	objective	evaluated.
Weakness statement	Specific observed deficiency	Prevents vague or cosmetic closure.
Affected assets / scope	Systems, users, applications, providers, locations	Shows where remediation must occur.
Root cause	Why the condition exists	Reduces recurrence.
Risk / operational impact	Security and business consequence	Supports prioritization.
Corrective action	What will change	Defines the remediation strategy.
Owner	Person accountable for completion	Creates management accountability.
Implementer	Team/provider performing technical work	Separates ownership from execution.
Milestones	Measurable intermediate results	Makes progress observable.
Dependencies	Licenses, vendors, change windows, approvals, hardware	Exposes schedule risk.
Scheduled completion	Target date	Creates time accountability.
Validation method	How effectiveness will be tested	Prevents closure based only on assertion.
Evidence	Artifacts proving completion	Supports closeout and future assessment.
Status	Open/in progress/blocked/validation/closed	Supports reporting.
Closure approval	Authorized reviewer/date	Establishes formal completion.

F.6 Writing the Weakness Statement

The weakness statement should describe the condition that exists, not merely repeat a requirement. A good statement identifies what is missing or ineffective and where it occurs. It avoids blaming a person before root-cause analysis has been performed. For example, “AC.L2-3.1.1 is not met” tells the remediation team almost nothing. “Quarterly access review records do not include the engineering enclave's local privileged accounts, and two former administrator accounts remain enabled on Server ENG-SRV-02” gives the team a condition it can investigate and correct.

The weakness statement should also distinguish evidence failure from implementation failure. If a control was operating but the organization cannot produce expected records, the remediation may involve evidence retention and governance. If the control was not operating, the remediation must correct the technical or procedural condition itself. The team should not manufacture retrospective evidence to make an implementation gap appear to have been satisfied.

F.7 Root-Cause Analysis

A POA&M that treats only the visible symptom often closes temporarily and reopens later. Root-cause analysis asks why the weakness occurred. Common causes include unclear responsibility, incomplete onboarding, unsupported technology, licensing gaps, undocumented exceptions, weak change control, provider assumptions, inadequate monitoring, staff turnover, training deficiencies, or a mismatch between policy and actual workflow.

Consider a missing EDR sensor. Reinstalling the sensor may correct one endpoint. Root-cause analysis may reveal that newly imaged laptops are not automatically enrolled in EDR because the provisioning workflow and RMM policy were never integrated. The durable corrective action is therefore larger than reinstalling one agent: the build process, enrollment automation, monitoring, exception workflow, and inventory reconciliation may all need correction.

F.8 Corrective Action Design

Corrective action should describe the future operating state. It should identify configuration changes, process changes, documentation updates, training, monitoring, and evidence procedures that are necessary to keep the weakness from returning. For complex findings, remediation should be treated as a miniature project rather than a single technician task.

The contractor remains responsible for deciding whether the corrective state is acceptable. The MSP can design and implement technical changes, the compliance specialist can map evidence and documentation, and a vendor can provide product support, but those roles do not eliminate contractor management responsibility for the system used to perform the contract.

F.9 Milestones Must Represent Outcomes

Milestones should be observable accomplishments. “Work on firewall” is not a milestone. “Approve revised enclave firewall rule standard,” “remove five identified overly broad rules,” “validate required application flows,” and “complete independent rule review” are milestones. Each milestone should have an owner, target date, completion criterion, and evidence source.

Milestones are especially important when remediation depends on several parties. A Microsoft tenant change may require customer approval, MSP configuration, a third-

party application update, user testing, and a change window. The POA&M should expose these dependencies rather than allowing the final due date to conceal them.

F.10 Dates, Aging, and the 180-Day CMMC Constraint

For internal remediation, management should establish target dates based on risk, complexity, business impact, and contractual obligations. For a valid CMMC Conditional status, however, the regulatory clock matters. Current DFARS and DoD CMMC information describe Conditional Level 2 status as limited to 180 days. A contractor should therefore plan closeout backward from the governing deadline and leave time for validation and the applicable closeout assessment process rather than scheduling the final technical change on day 180.

A useful management practice is to establish internal warning thresholds well before the external deadline. For example, management may require executive review at 30, 60, 90, and 120 days, with increasingly frequent escalation for unresolved items. These are internal governance checkpoints, not substitutes for the official CMMC timing rules.

F.11 Evidence-Based Closure

A weakness is not closed because a technician marks a ticket complete. Closure requires evidence that the corrective action has been implemented and that the applicable condition is now satisfied. Evidence may include configuration exports, access-review records, screenshots with context, scan results, log records, policy approvals, tickets, test results, restored files, system inventories, or other artifacts appropriate to the requirement.

The validator should be able to reproduce or independently confirm the result. If the POA&M concerned missing log ingestion, the team should not close it after restarting the collector. It should demonstrate that required sources are arriving, timestamps and parsing are correct, retention is functioning, monitoring detects ingestion failure, and the operational procedure has been updated where necessary.

F.12 Relationship to Tickets, Projects, and Change Management

The POA&M should not replace the MSP's PSA, project platform, or change-management system. The POA&M is the compliance and management record; technical work can be executed through linked tickets and changes. This keeps

technician-level details in the operational platform while preserving an executive and assessment-ready view of the remediation.

Every POA&M item should therefore have traceable identifiers for related tickets, changes, projects, vendor cases, and evidence. When a ticket is closed, the POA&M may remain in validation. When the POA&M is closed, the evidence package should show the complete chain from finding to correction to verification.

F.13 Responsibility Model for POA&M Remediation

Appendix C's responsibility model applies directly. The contractor owns the compliance decision and should designate the accountable remediation owner. The MSP may implement technical corrections. An MSSP may validate monitoring changes. A cloud provider may resolve a service issue. A readiness specialist may help organize evidence. The assessor performs the applicable assessment or closeout role; the assessor should not be converted into the contractor's implementation team.

The POA&M should make these boundaries explicit because remediation often fails at handoffs. If the customer must approve a license purchase before the MSP can deploy a feature, that approval is a milestone and dependency. If the MSP expects the customer to validate a business workflow, that responsibility must have an owner and date.

F.14 Worked Example — Identity and MFA

Party ABC discovers that several legacy administrative workflows rely on authentication paths that do not meet the approved identity design. The weakness affects privileged access and cannot be treated as a simple checkbox. The remediation team first identifies every affected account, application, authentication method, owner, and dependency. It then determines which accounts can be eliminated, which applications must be modernized, and which service identities require a different non-interactive authentication design.

Milestone	Owner / Implementer	Target	Completion Evidence
Inventory affected identities and applications	ABC IT owner / Party IJK MSP	Day 10	Approved inventory and dependency map
Approve replacement authentication design	ABC security owner	Day 25	Architecture approval
Acquire/assign required licensing	ABC procurement / MSP support	Day 35	License assignment report
Pilot replacement configuration	MSP identity engineer	Day 55	Pilot results and sign-in evidence
Production cutover	MSP + application owner	Day 75	Change record and configuration

Milestone	Owner / Implementer	Target	Completion Evidence
			export
Disable legacy paths	MSP	Day 80	Account/authentication records
Independent validation	ABC security/compliance	Day 90	Validation record and evidence package

The example illustrates why a single due date is insufficient. The license decision, application dependency, pilot, cutover, removal of the old path, and independent validation are separate outcomes. If one dependency slips, management can see the effect before the final deadline is endangered.

F.15 Worked Example — Vulnerability and Patch Remediation

Party ABC's authenticated vulnerability scan identifies a high-impact weakness on an engineering application server. The vendor patch is available, but the server supports a production workflow and cannot be restarted during normal operations. The POA&M records the vulnerability, affected asset, exposure, vendor advisory, business owner, maintenance-window dependency, backup requirement, patch test, production deployment, rescan, and closure evidence.

The MSP should not close the item when the patch package reports success. The validation milestone requires a rescan or equivalent technical verification showing that the identified condition is no longer present. If the patch creates an operational problem and must be rolled back, the POA&M remains open and the revised strategy is documented.

F.16 Worked Example — SIEM Log Source Failure

Party IJK operates the SIEM for Party ABC. During a monthly evidence review, the team discovers that a domain controller stopped forwarding security logs twelve days earlier. The immediate action is to restore ingestion, but the POA&M asks the larger question: why did twelve days pass without detection?

Root-cause analysis shows that alerting existed for security events but not for log-source health. Corrective action therefore includes restoration of forwarding, review of the missing period, creation of ingestion-health monitoring, escalation thresholds, PSA ticket automation, a daily SOC check, and evidence demonstrating that a simulated interruption generates the expected alert. This converts a one-time repair into a sustainable control improvement.

F.17 Worked Example — Backup Restoration Failure

A scheduled restore test fails even though daily backup jobs have been reporting success. The POA&M should not be written as “backup failed.” It should identify the protected workload, backup repository, recovery point selected, error condition, business impact, and whether other recovery points or systems may be affected.

Remediation may require correcting permissions, storage configuration, encryption keys, application-consistent backup settings, or retention. Closure requires a successful restoration and validation of recovered data, followed by an update to the recurring restore-test procedure if the root cause exposed a process weakness.

F.18 Worked Example — Documentation and Implementation Mismatch

Party EGH's SSP states that privileged accounts are reviewed quarterly, but interviews and records show that only standard user accounts are included in the review. The team should not solve this by editing the SSP to remove the statement unless that reflects the intended and compliant operating model. Instead, it determines the applicable requirement, identifies the missing privileged-account population, updates the access-review procedure, performs the review, corrects discovered access issues, and preserves evidence.

This example teaches a critical principle: remediation is not the art of making documentation match a weak environment. Documentation and the operating environment should converge on the required, approved, and sustainable practice.

F.19 Party ABC — Existing Contractor Remediation Scenario

Party ABC is already performing DoD work. Its readiness review produces a mixture of technical findings, documentation inconsistencies, evidence gaps, and provider-responsibility ambiguities. ABC establishes an internal remediation register immediately rather than waiting for an assessment. Management separates quick corrections from structural projects and identifies which findings could jeopardize assessment readiness.

ABC assigns an executive remediation owner, a security/compliance coordinator, system owners, and Party IJK as the principal MSP implementer. Weekly technical meetings review milestones and blockers. Monthly management reviews examine

aging, budget, scope changes, and evidence. The goal is to reach the formal assessment with no reliance on a POA&M where avoidable.

F.20 Party EGH — Prospective Offeror Scenario

Party EGH has not yet received CUI and is designing its environment. Its POA&M-like internal remediation register is used during implementation to track incomplete architecture work: government-cloud tenant configuration, managed endpoints, centralized logging, EDR deployment, backup testing, policy approval, and user training. Because EGH is still building, many entries are project gaps rather than post-assessment deficiencies.

This is an ideal time to eliminate weaknesses. EGH should avoid treating the future availability of Conditional status as an implementation strategy. The objective is to complete, test, document, and evidence the environment before it becomes dependent on a contract award timeline.

F.21 Party IJK — MSP Remediation Operating Model

Party IJK needs a repeatable method for managing remediation across customers without confusing MSP tickets with customer compliance ownership. IJK creates a POA&M support service that can maintain technical milestones, evidence links, dependency tracking, and reporting while leaving formal compliance ownership with the customer.

For every item, IJK identifies whether the action is included in the managed-service agreement, requires a project, requires new licensing, depends on another provider, or requires customer action. This classification prevents a common failure in which a remediation item remains open because each party assumed the other party was responsible for funding or performing it.

F.22 POA&M Status Model

Status	Meaning	Required Management Behavior
Open	Finding accepted; remediation not yet started	Assign owner, strategy, dates, dependencies.
In Progress	Corrective work underway	Track milestones and blockers.
Blocked	Progress cannot continue	Identify blocker owner; escalate quickly.
Pending Validation	Technical work complete; effectiveness not yet verified	Perform independent validation and collect evidence.
Ready for Closeout	Internal validation complete	Prepare applicable closeout package/process.

Status	Meaning	Required Management Behavior
Closed	Authorized validation/closeout complete	Lock evidence, record closure date, update SSP/processes if needed.
Reopened	Closure proved ineffective or condition recurred	Perform new root-cause analysis and corrective action.

F.23 Aging and Escalation Dashboard

Age / Threshold	Internal Management Action	Questions to Ask
0–30 days	Owner and plan confirmed	Is scope understood? Are dependencies funded?
31–60 days	Management review	Are milestones on schedule? Has evidence collection begun?
61–90 days	Executive visibility for material items	What could prevent closure? Is vendor escalation needed?
91–120 days	Recovery plan and increased review cadence	Is the current strategy still credible?
121–150 days	Senior escalation for any formal 180-day-bound item	Is validation/closeout time protected?
151–180 days	Immediate executive management for formal conditional items	Has applicable closeout been completed before status expires?

These thresholds are recommended internal governance examples, not regulatory deadlines other than the separately applicable 180-day limit for current Conditional CMMC status. An organization may adopt more aggressive thresholds.

F.24 Management Review Questions

- Does every open item have one accountable owner?
- Is the weakness statement specific enough to validate?
- Has root cause been distinguished from the visible symptom?
- Are technical and business dependencies identified?
- Are required licenses, hardware, professional services, and change windows funded?
- Are milestones outcome-based and dated?
- Is the affected CMMC scope understood?
- Has the SSP, network/data-flow documentation, policy, or responsibility matrix been updated when necessary?
- Is evidence being collected during remediation rather than reconstructed later?
- Is any formal Conditional-status item approaching the applicable 180-day limit?
- Has the contractor distinguished internal remediation from formal CMMC POA&M eligibility?

- Can management explain why each item remains open and what will cause it to close?

F.25 Completed Sample POA&M

ID	Weakness	Root Cause	Corrective Action	Owner	Milestones / Target	Validation / Evidence	Status
ABC-001	Two former privileged accounts remain enabled on an enclave server.	Termination workflow covered cloud identity but not local server accounts.	Integrate local privileged-account inventory into termination and quarterly review; disable accounts; validate all enclave systems.	ABC Security Manager	Inventory D10; disable D15; workflow update D25; review D35	Disabled-account evidence; revised procedure; completed access review	Pending Validation
ABC-002	One critical log source stopped forwarding to SIEM without alert.	No ingestion-health monitoring for that source class.	Restore forwarding; implement health alert; automate ticket; test interruption.	IJK SOC Lead	Restore D2; monitor D10; test D15	SIEM ingestion record; simulated failure alert; PSA ticket	In Progress
ABC-003	Restore test failed for engineering file repository.	Backup job success was monitored, but recovery configuration was not validated after storage change.	Correct recovery permissions/configuration; repeat restore; update change checklist.	IJK Backup Lead / ABC System Owner	Root cause D7; fix D14; restore D21	Successful restore record; integrity check; revised checklist	Open

F.26 Blank Reusable POA&M Template

POA&M ID	Requirement / Objective	Weakness	Affected Scope	Root Cause	Corrective Action	Owner	Implementer	Milestones	Dependencies	Target Date	Validation	Evidence	Status

F.27 Milestone Detail Worksheet

POA&M ID	Milestone #	Outcome	Owner	Start	Target	Dependency	Evidence	Complete

POA&M ID	Milestone #	Outcome	Owner	Start	Target	Dependency	Evidence	Complete

F.28 POA&M Closure Package

A mature closure package should allow a reviewer to understand the original condition, the corrective strategy, the work performed, and the evidence that demonstrates the new state. It should preserve the original finding rather than overwriting history. The package normally includes the POA&M record, linked change/ticket records, relevant configuration or technical evidence, validation results, updated procedures or SSP sections where applicable, approval, and closure date.

For a formal CMMC POA&M, the organization must follow the applicable CMMC closeout assessment process rather than treating its internal closure approval as the official Final-status action. The internal package prepares the organization to demonstrate remediation; it does not replace the required assessment mechanism.

F.29 POA&M Change Control

POA&M records themselves require change control. If the target date, strategy, scope, owner, or milestone sequence changes, the record should preserve who approved the change and why. Repeated date movement without documented cause is a warning sign that the corrective strategy may not be viable.

A change to architecture during remediation may also change assessment scope. For example, moving CUI to a new cloud service to solve one weakness can introduce a new ESP, new identities, new data flows, new security protection assets, and new evidence responsibilities. The remediation team should therefore coordinate POA&M changes with the SSP, asset inventory, data-flow diagrams, provider register, and Appendix C responsibility matrix.

F.30 Reporting to Executives

Executives generally need a different view from technicians. A management report should show total open items, aging, critical blockers, items affecting assessment readiness, budget or procurement dependencies, provider dependencies, overdue milestones, items pending validation, and trends. It should not bury leadership in raw scanner output.

For formal Conditional status, executives also need explicit visibility into the remaining regulatory time window. The affirming official and senior management should understand that failure to close a valid POA&M within the permitted period affects the organization's ability to maintain the required Final CMMC status.

F.31 Reporting From the MSP to the Contractor

The MSP's remediation report should distinguish work completed from compliance closure. It can say that a patch was deployed, a configuration changed, or an EDR sensor restored. The contractor or applicable assessment process determines whether the POA&M item is ready for or has achieved formal closure.

The MSP should also report customer dependencies plainly. If remediation is waiting on a license purchase, application-owner testing, legal approval, downtime authorization, or another provider, the report should identify the dependency, responsible party, date requested, and effect on the schedule.

F.32 What Not to Put on a POA&M

A POA&M should not become a warehouse for every help-desk ticket, routine maintenance task, low-value observation, or future enhancement. Overloading the register hides the weaknesses that require management attention. Organizations should maintain separate operational backlogs and link them when they support a POA&M milestone.

More importantly, a formal CMMC assessment POA&M cannot be used merely because management would prefer more time. Eligibility is controlled by the CMMC rule. Level 1 does not permit POA&Ms, and Level 2 POA&M use is limited. Readers should verify the current rule before assuming that a particular unmet requirement may remain open at the time of assessment.

F.33 Common POA&M Failure Patterns

Common failure patterns include vague weakness statements, no root-cause analysis, a single final due date with no milestones, owners who lack authority, dependencies discovered late, evidence collected only after the fact, technical tickets closed before validation, repeated date extensions, and documentation left inconsistent with the remediated environment.

Another serious failure is confusing a product purchase with remediation. Buying a SIEM does not close a logging weakness until required sources are onboarded, monitored, retained, and tested. Buying MFA licensing does not close an authentication weakness until the required identities and access paths are actually protected and the result is validated.

F.34 Pre-Assessment Use of the POA&M Method

The strongest use of this appendix occurs before the formal assessment. A readiness team can apply the POA&M structure to every material gap discovered during internal review. This creates disciplined remediation without relying on formal Conditional status. By assessment time, the organization should be able to show that weaknesses were identified, corrected, validated, and incorporated into normal operations.

This approach also improves management credibility. The organization is not presenting a last-minute compliance project; it is demonstrating an operating remediation system that discovers and corrects weaknesses continuously.

F.35 Final POA&M Standard

A POA&M is acceptable for management purposes only when another qualified person can read it and determine what is wrong, why it happened, what will be done, who is responsible, when measurable outcomes are due, what dependencies threaten completion, how effectiveness will be validated, and what evidence will prove closure.

For CMMC purposes, add one more question: is this item actually eligible for formal POA&M treatment under the current CMMC rule? That question must be answered from authoritative requirements, not from habit, vendor marketing, or a generic cybersecurity template.

F.36 2026 Regulatory Verification Note

This teaching edition was prepared using the CMMC rules and DoD acquisition material current in September 2026. DFARS 252.204-7021 (NOV 2025) defines a POA&M as a document identifying tasks, required resources, milestones, and scheduled completion dates; requires a contractor with Conditional CMMC Status to successfully close a valid POA&M to achieve Final status; and defines current Conditional Level 2 status as not older than 180 days, subject to the clause's

conditions. DFARS Subpart 204.75 also states that CMMC Levels 2 and 3 can be conditional for a period not exceeding 180 days, while Level 1 requires Final status for award.

DoD's current CMMC program page states that Level 1 POA&Ms are not permitted and that Level 2 POA&Ms are permitted only as defined by 32 CFR 170.21 and must be closed within 180 days. Because CMMC implementation guidance and acquisition rules can change, the final publication and every real assessment should recheck 32 CFR part 170, current DFARS clauses, and current DoD CMMC guidance.

F.37 Building the POA&M From an Assessment Finding

A remediation record should begin with the actual finding, not a technician's shortened interpretation. Preserve the requirement identifier, assessment objective or finding reference, date identified, affected scope, and the evidence that led to the finding. The remediation team can then translate the finding into operational language: what behavior must change, what process must be repaired, what documentation must be updated, and what evidence will demonstrate the corrected state.

The team should also determine whether the visible finding is localized or systemic. One unauthorized local administrator account, for example, should trigger a review of the provisioning process and the wider population of comparable systems. Closing one account without testing the population may correct the symptom while leaving the root cause intact.

F.38 POA&M Eligibility Before Conditional-Status Planning

A contractor should evaluate formal POA&M eligibility before building an assessment schedule around Conditional status. The practical rule is that an organization should never assume every remaining gap can be deferred. The readiness team should record whether an item appears eligible, what authoritative rule supports that conclusion, who verified it, and when it was verified.

If eligibility is uncertain, the safer planning assumption is that the item must be completed before assessment. This is especially important for MSPs because a provider may view a technical issue as ordinary backlog work while the contractor faces a contractual CMMC-status deadline.

F.39 Prioritization Without Inventing a Compliance Score

Internal prioritization should consider assessment significance, cybersecurity risk, business impact, remediation complexity, and schedule dependency. These dimensions should remain visible rather than being collapsed into an invented compliance score. A documentation inconsistency may have modest immediate technical risk but high assessment significance; a legacy application may create severe schedule risk because remediation depends on vendor development.

Management should therefore see why an item is prioritized, what will happen if it slips, and which other milestones depend on it. The official CMMC assessment treatment remains governed by the applicable methodology and rules.

F.40 Remediation Work Breakdown Structure

Large items should be decomposed into a work breakdown structure. The top-level corrective action defines the intended future state; milestones represent major outcomes; linked project tasks and tickets contain technician-level work. Typical phases include discovery, design, approval, procurement, implementation, testing, documentation, training, evidence collection, independent validation, and closeout preparation.

This structure keeps the POA&M readable for management while preserving traceability to detailed operational work. The POA&M should link to tickets rather than duplicate every technician note.

F.41 Dependency Management

Dependencies are a primary cause of missed remediation dates. Common dependencies include customer approval, procurement, licensing, hardware delivery, vendor support, maintenance windows, application testing, legal review, facility access, subcontractor action, or completion of another remediation item.

Each dependency should have an owner and a required-by date. 'Waiting on customer' is not adequate. The record should identify the exact decision or resource required, who can provide it, when it was requested, and the effect of delay on downstream milestones.

F.42 Budget and Procurement

Some weaknesses require licenses, replacement hardware, professional services, new circuits, cloud subscriptions, or application modernization. The POA&M should expose these costs early and identify funding status, procurement owner, lead time, renewal implications, and whether the purchase introduces a new provider or scope relationship.

Purchase is only an enabling milestone. Buying a security product does not close a weakness until the product is configured, operated, tested, and evidenced in the affected environment.

F.43 Exceptions, Risk Acceptance, and POA&M

An exception is an authorized deviation from an internal standard. Risk acceptance is a governance decision to acknowledge a risk. A POA&M is a plan to correct a deficiency. These concepts should not be used interchangeably.

An internal exception or risk acceptance does not automatically satisfy a CMMC requirement or make an unmet assessment objective eligible for formal POA&M treatment. Temporary exceptions used during remediation should have owners, expiration dates, and links to the corrective-action record.

F.44 Evidence Planning at the Beginning

Evidence planning should occur when corrective action is designed. For each milestone, determine what artifact will prove completion, who will generate it, where it will be stored, how long it will remain available, and who will validate it. This prevents technically completed work from becoming an evidence problem later.

Evidence should be authoritative and proportionate. Configuration exports and system-generated reports are often stronger than isolated screenshots. Tickets establish chronology and approval but may not prove technical state. Strong closure packages combine governance, implementation, and operational evidence.

F.45 Independent Validation and Separation of Duties

When practical, the implementer should not be the only person who decides remediation is effective. A second engineer, security lead, system owner, or qualified reviewer can independently test the corrected condition. This catches incomplete changes and improves credibility.

For formal CMMC closeout, the applicable assessment process remains controlling. Internal validation prepares the organization; it does not replace required closeout activity.

F.46 Reopening a Closed Item

An item should be reopened when the condition returns, a system change recreates the weakness, or later evidence shows that the assumed root cause was incomplete. The record should preserve the original closure history and explain why the earlier corrective action did not remain effective.

Repeated reopening is a management signal that the organization may be correcting symptoms rather than processes, that ownership is unclear, or that the selected technology cannot reliably support the intended control.

F.47 Integration With the SSP and Supporting Documentation

If remediation changes how a requirement is implemented, the SSP should be reviewed and updated as appropriate. New providers, network segments, cloud services, identity flows, or evidence systems may also require updates to diagrams, inventories, data-flow documentation, policies, procedures, and the Appendix C responsibility matrix.

Closing a technical item while leaving outdated documentation creates the next assessment problem. The corrected environment and its governing documentation should converge before closure.

F.48 SPRS and Affirmation Relationships

CMMC status, assessment results, SPRS records, and affirmations involve official systems and organizational roles that are distinct from the MSP's remediation tracker. The contractor should designate responsibility for official actions. The MSP can provide technical evidence and status information but should not assume authority that belongs to the contractor.

Operational reports should avoid implying that a technician's closure action automatically changes official CMMC status. Formal status follows the applicable assessment, closeout, affirmation, and system-of-record processes.

F.49 Closeout Assessment Preparation

Preparation for a formal closeout should begin well before the end of the permitted period. Assemble the original finding, remediation plan, milestone history, technical evidence, validation results, updated documentation, and relevant provider records. A reviewer should be able to trace the complete path from deficiency to corrected state.

The contractor should also confirm that the environment being presented is the environment that was remediated. Major architecture changes during remediation may require renewed scoping analysis.

F.50 Managing the 180-Day Window

A 180-day maximum should not be managed as one undifferentiated block. An internal plan can reserve days 1–30 for ownership, root cause, design, funding, and dependencies; days 31–75 for procurement and implementation; days 76–120 for production completion and documentation; and days 121–150 for validation, evidence completeness, and residual corrections. The remaining time should be protected for closeout and contingency.

This is an internal planning model, not a substitute for the governing rule. The lesson is to avoid scheduling normal implementation to consume the entire Conditional-status period.

F.51 Weekly and Monthly Review Structure

A weekly remediation meeting should focus on milestone completion, blockers, upcoming changes, evidence, and decisions required before the next meeting. Owners should explain variance rather than merely read status fields.

A monthly management review should focus on aging, assessment significance, budget, provider dependencies, items approaching critical dates, and systemic trends. Even when the same people attend both meetings, technical execution and management oversight should remain distinct.

F.52 MSP Service Commitments for Remediation

When an MSP performs corrective work, the service agreement should distinguish recurring managed-service work from separately scoped projects. Otherwise, the customer may believe a CMMC remediation is included while the MSP considers it out-of-scope engineering.

The POA&M should identify resource requirements, escalation paths, and customer dependencies. High-impact remediation may require dedicated engineering or project management rather than placement in a normal help-desk queue.

F.53 External Provider and Subcontractor Remediation

A weakness may depend on a cloud provider, SOC, backup provider, application vendor, or subcontractor. The POA&M should identify the external party, provider case, contractual mechanism, customer owner, escalation path, expected evidence, and contingency if the provider cannot meet the schedule.

If a provider cannot structurally support the required operating state, remediation may require replacement of the service. That decision can introduce migration, licensing, scope, contract, and evidence consequences.

F.54 Full Case Study — Party ABC

Party ABC discovers that several enclave workstations are missing the approved endpoint baseline, one is not reporting to EDR, and the asset inventory contains outdated ownership. Rather than treating these as isolated tickets, ABC and Party IJK investigate the provisioning process. They discover that a temporary imaging method bypassed normal management enrollment and identify seven affected systems.

The remediation plan inventories the complete population, enrolls devices, applies the baseline, validates encryption and host firewall settings, restores EDR coverage, reconciles ownership, tests policy enforcement, and updates the build procedure. IJK also adds monitoring for devices missing required agents. Closure evidence includes the original finding, affected-device inventory, policy reports, EDR health records, revised procedure, change records, and independent validation. The durable result is not simply seven repaired devices; the provisioning process that created the weakness is corrected.

F.55 Full Case Study — Party EGH

Party EGH performs a mock assessment before its first formal assessment and finds incomplete log retention, inconsistent privileged-account review, missing restore-test evidence, and SSP statements that describe planned rather than implemented practices. EGH creates an internal remediation program instead of assuming these items can remain open at assessment.

Party IJK configures required log sources and retention, implements ingestion-health monitoring, and produces validation reports. EGH expands privileged-account review across cloud, local, network, and service-administration populations. The backup team performs documented restores. The compliance lead revises the SSP only after corrected processes operate. Management bases readiness decisions on evidence, not percentage-complete estimates.

F.56 Full Case Study — Party IJK

Party IJK supports multiple defense contractors and maintains a separate remediation register for each customer plus a provider-level engineering backlog for shared-service weaknesses. A defect in a shared RMM or SOC service can be linked to affected customer records without exposing one customer's information to another.

IJK standardizes status definitions, evidence packaging, and escalation rules. It distinguishes customer-funded projects from recurring service work and reviews cross-customer trends to identify provider-level root causes. This converts repeated customer findings into improvements in the MSP's own service architecture.

F.57 Executive Dashboard Structure

Executives should receive a concise remediation dashboard showing open items, aging, blocked items, overdue milestones, items pending validation, customer and provider dependencies, budget requirements, formal Conditional-status items, closures, and reopened items. The dashboard should highlight decisions required from leadership rather than reproduce raw scanner output.

Trend information matters. A falling number of open items can be positive, but repeated reopening or growing average age may indicate weak root-cause correction. Management should look at the health of the remediation system, not only the count.

F.58 Detailed Closeout Standard

Before closure, confirm that the original finding is preserved; affected scope is complete; root cause is addressed; corrective action is implemented; milestones are complete; dependencies and temporary exceptions are resolved; technical validation is successful; evidence is stored with provenance; linked tickets and changes are traceable; and supporting documentation has been updated.

For formal CMMC POA&M items, internal closure is not the same as official closeout. The applicable CMMC closeout assessment and status process must be completed.

F.59 POA&M Record Quality Test

A qualified person who did not participate in remediation should be able to read the record and understand the original problem, corrective logic, milestone history, evidence, validation, and reason for closure. If tribal knowledge is required to interpret the record, it is incomplete.

This test discourages vague abbreviations, unexplained ticket references, unsupported status claims, and evidence folders that cannot stand on their own.

F.60 Closing Perspective

The value of a POA&M is not the spreadsheet. Its value is the discipline it imposes on remediation: accountable ownership, root-cause analysis, measurable milestones, dependency management, evidence, validation, and closure. Used continuously, this discipline reduces the number of unresolved weaknesses that reach a formal assessment.

For contractors, the process creates management visibility. For MSPs, it converts compliance gaps into executable technical work while documenting customer dependencies. Formal CMMC POA&M eligibility and closeout, however, remain governed by the current CMMC rules.

F.61 Expanded Remediation Review Checklist

- Finding language and requirement reference preserved.
- Formal POA&M eligibility verified separately from internal remediation.
- Complete affected population identified.
- Root cause documented.
- Corrective state clearly defined.
- Owner and implementer identified.
- Milestones are measurable outcomes.
- Dependencies have owners and required-by dates.
- Funding and procurement status known.
- Evidence planned before implementation.
- Independent validation assigned where practical.

- SSP and supporting documentation impacts reviewed.
- Provider and subcontractor dependencies documented.
- Official CMMC closeout/status actions distinguished from internal ticket closure.
- Recurrence-prevention action incorporated into normal operations.

Deepening Note — Formal POA&M Eligibility and Assessment Strategy

The organization should treat formal POA&M eligibility as an assessment decision governed by 32 CFR 170.21, not as an internal project-management preference. DoD's current CMMC material distinguishes Operational Plans of Action used for ordinary maintenance and risk management from CMMC POA&Ms associated with Conditional status. This distinction should be built into the contractor's governance language so that technicians do not casually describe every remediation ticket as a CMMC POA&M.

Before the assessment, the readiness team should identify every known unmet or uncertain objective and ask three separate questions. First, can the weakness be corrected before the assessment? Second, if it remains, is formal POA&M treatment actually permitted by the current rule? Third, if Conditional status is achieved, can the organization realistically implement, validate, and complete the required closeout process within the available period? A “yes” to the second question does not automatically produce a “yes” to the third.

The preferred readiness strategy is therefore to enter the assessment with as few unresolved conditions as practical. Conditional status is a limited remediation mechanism, not a substitute for completing the security program.

Deepening Note — What Happens During the Closeout Sequence

The closeout sequence should be taught as a chain rather than a final meeting. The chain begins when the organization receives Conditional status with a valid POA&M. The remediation team freezes the authoritative list of open items, assigns owners, confirms eligibility and deadlines, and creates an evidence plan. Technical teams perform the corrective work while management monitors milestones and dependencies. Qualified reviewers validate the corrected state before the organization initiates the applicable POA&M closeout assessment.

For a Level 2 self-assessment, DoD states that the POA&M closeout self-assessment is performed by the Organization Seeking Assessment in the same manner as the

initial self-assessment. For a Level 2 certification assessment, the applicable closeout is conducted through the C3PAO process. The organization should preserve the distinction between its internal validation and the formal closeout activity.

DoD's March 2026 CMMC FAQ adds an important operational consequence: during the 180-day Conditional period, a POA&M Closeout Assessment can be finalized in CMMC eMASS only once. If one or more required security requirements remain NOT MET when that closeout is finalized, the Conditional status is terminated and the organization must begin again with a new assessment to achieve CMMC status. If the closeout is not finalized within 180 days of the CMMC Status Date, the Conditional status automatically expires. This makes premature closeout a serious governance error. The contractor should initiate final closeout only after its internal validation demonstrates that the POA&M is actually ready.

Deepening Note — The 180-Day Clock as a Project Constraint

The 180-day period should be managed as a hard external constraint with an earlier internal completion target. Management should not plan to use all 180 days for engineering. The organization needs time for failed tests, vendor delays, evidence corrections, documentation alignment, management review, and the formal closeout process.

A practical internal schedule can target technical implementation by approximately day 100–120, complete independent validation and evidence reconciliation by approximately day 135–145, and preserve the remaining period for closeout and contingency. These are internal management targets, not regulatory deadlines. A simple infrastructure correction may finish far earlier; a complex application migration may require an even more aggressive start.

At each review, the team should calculate remaining calendar time, not merely percentage complete. A project that reports 80 percent complete on day 150 may be in worse condition than a project that reports 60 percent complete on day 60. The critical question is whether the remaining work, validation, and closeout can credibly finish before Conditional status expires.

Deepening Note — Assessment Scoring and Remediation Planning

The remediation team should preserve the official assessment score and requirement treatment from the applicable CMMC assessment methodology. Internal dashboards

may add risk and project information, but they should not alter the official meaning of an assessment result or invent a replacement scoring system.

Scoring information is useful because it helps the team understand the assessment consequence of a NOT MET requirement and whether the overall result meets the conditions for Conditional status. But remediation planning should go beyond the numeric value. The team must understand the technical dependency represented by the finding. A requirement with a particular assessment value may be connected to several systems, users, or providers, and its remediation may require architecture work that is not obvious from the score alone.

For that reason, the POA&M record should contain the official assessment reference and score treatment where applicable, while the project plan separately captures engineering complexity, risk, cost, dependency, and schedule. Keeping those concepts separate prevents management from assuming that a low numerical weight necessarily means an easy or low-risk remediation.

Deepening Note — SPRS, CMMC UID, and Affirmation Workflow

The official status workflow should be separated from the MSP's technical workflow. DFARS 252.204-7021 requires the contractor to maintain the applicable current CMMC status for systems used in contract performance that process, store, or transmit FCI or CUI; provide applicable CMMC UIDs to the contracting officer; enter required self-assessment results in SPRS when applicable; and complete annual affirmations of continuous compliance in SPRS for each applicable CMMC UID.

The affirming official is therefore not merely signing an MSP project report. The affirmation concerns continuous compliance associated with the required CMMC level. The contractor should establish an internal evidence review before the affirmation so the responsible official has a reasonable basis for the action. The MSP should provide current technical evidence, exceptions, unresolved remediation, major changes, and scope information needed by contractor management.

When Conditional status is involved, the remediation dashboard should show the CMMC Status Date, the applicable CMMC UID, the official status type, the internal target closeout date, the 180-day expiration date, the responsible affirming official, and the party responsible for coordinating the applicable closeout assessment. This prevents regulatory administration from becoming disconnected from engineering remediation.

Deepening Note — A Day-by-Day Example of a Conditional Level 2 Remediation

Assume Party ABC receives Conditional Level 2 status on January 10 after an assessment identifies eligible unresolved items. Day 0 is not a waiting period; it is the beginning of the closeout project. Within the first several business days, ABC confirms the authoritative POA&M, assigns an executive owner, validates every technical owner and provider dependency, and establishes an internal completion target substantially earlier than the external expiration.

During days 1–15, Party IJK performs detailed discovery and confirms the complete affected populations. ABC approves the remediation architecture and any required funding. During days 16–45, licenses, vendor changes, and technical prerequisites are completed. Pilot changes are tested before broad production deployment. Evidence collection begins immediately.

During days 46–90, the primary production remediation is completed. Any failed implementation is treated as schedule variance and escalated. The SSP, procedures, diagrams, inventories, and responsibility matrix are updated as the new operating state becomes stable. During days 91–120, ABC performs full-population validation, not merely sample spot checks where complete validation is feasible. Recurring processes such as access reviews or monitoring are allowed enough time to demonstrate operation.

During days 121–145, a reviewer who was not the primary implementer walks every POA&M item from original finding through evidence. Missing artifacts, inconsistent documentation, and residual technical conditions are corrected. Management then conducts a formal readiness-to-close review. The closeout process is coordinated only when ABC has evidence that every required item is ready.

The remaining period is contingency. ABC does not intentionally wait until the final days. If a provider outage, failed test, or evidence issue appears, management still has time to respond. This example illustrates the central principle: the external 180-day maximum should produce an internal schedule that finishes materially earlier.

Deepening Note — Fully Worked POA&M Record: Privileged Access

Finding: Party ABC's enclave uses named administrator accounts for most privileged activity, but two infrastructure systems still permit routine administration through

shared local administrator credentials. The assessment evidence shows that individual accountability is incomplete for those systems.

Root cause: The systems were deployed before the current privileged-access standard. They were excluded from centralized identity because an application vendor warned that changing the authentication method might affect support. The exception was never assigned an expiration date, and the quarterly privileged-account review did not include the local accounts.

Corrective strategy: ABC and Party IJK first confirm application support requirements with the vendor. IJK creates named administrative identities using the approved authentication architecture, tests application functionality, removes routine use of shared credentials, places any required emergency credential under controlled break-glass procedures, expands the quarterly access review population, and updates the privileged-access procedure.

Milestones: vendor compatibility confirmation; approved design; test identities; pilot; production migration; shared-credential restriction; access-review update; independent validation; documentation update. Dependencies include vendor support and a production maintenance window.

Closure evidence: vendor case or compatibility record, approved change, identity configuration, role assignments, authentication logs, evidence that shared routine use is disabled, revised access-review population, completed review record, updated procedure, and independent validation results. The item remains in Pending Validation until the reviewer demonstrates that privileged actions are attributable to named identities and the recurring review includes the affected systems.

Deepening Note — Fully Worked POA&M Record: Vulnerability Management

Finding: Authenticated scanning identifies a critical vulnerability on an engineering server. The patch exists, but the application owner has deferred installation for three maintenance cycles because of production concerns.

Root cause: The vulnerability-management procedure assigns scanning to the MSP but does not establish who has authority to accept downtime, who escalates overdue remediation, or what happens when an application owner repeatedly defers a patch. The weakness is therefore both technical and governance-related.

Corrective strategy: ABC assigns the system owner authority to schedule the maintenance window, IJK creates a tested backup and rollback plan, the application vendor confirms patch compatibility, the patch is deployed, and the system is rescanned. ABC also revises the vulnerability procedure to define escalation thresholds and documented exception handling.

Closure evidence includes the original authenticated scan, vendor advisory, maintenance approval, backup/rollback evidence, change record, patch result, post-change health check, authenticated rescan showing the identified condition is resolved, revised procedure, and management approval. A patch deployment message alone is insufficient.

Deepening Note — Fully Worked POA&M Record: Logging and SOC

Finding: A critical Windows log source stopped reporting to the SIEM for twelve days without generating a health alert. Security events from that system were therefore unavailable to normal SOC monitoring during the interruption.

Root cause: The SIEM implementation monitored security detections but did not monitor expected log-source heartbeat. The MSP's onboarding checklist verified ingestion at installation but did not create a recurring health test.

Corrective strategy: IJK restores ingestion, determines the period of missing telemetry, evaluates whether alternate evidence exists for the gap, implements heartbeat monitoring, creates an automated PSA ticket for prolonged ingestion failure, documents escalation thresholds, and updates the SIEM onboarding standard so every critical source receives a health monitor.

Validation deliberately interrupts a test source and confirms that the SIEM detects the failure, creates the expected alert/ticket, and routes it to the correct SOC queue. Closure evidence includes restored ingestion, configuration, alert test, ticket, revised onboarding procedure, and reviewer signoff. This demonstrates both correction and recurrence prevention.

Deepening Note — Fully Worked POA&M Record: Backup and Recovery

Finding: The engineering file repository reports successful nightly backups, but the quarterly restore test fails because the recovery account no longer has access to the required encryption key.

Root cause: A security hardening change rotated privileged credentials and encryption-key access, but the backup recovery workflow was not included in the change-impact review. Backup-job success continued because writing new backups did not require the same recovery operation.

Corrective strategy: IJK restores the approved recovery access path, reviews key custody and break-glass procedures, performs a successful restore to an isolated location, validates file integrity and permissions, updates the change checklist to include backup/recovery dependencies, and schedules an additional follow-up restore test.

The closure package includes failed-test evidence, root-cause analysis, approved access changes, successful restoration records, integrity validation, revised key-custody and change procedures, and follow-up test scheduling. The example demonstrates why 'backup successful' and 'recoverability validated' are different statements.

Deepening Note — Management Decision Gate Before Closeout

Before the organization authorizes the formal closeout step, senior management should conduct a decision gate. The purpose is not to redo the technical assessment but to confirm that the organization is not prematurely consuming its closeout opportunity.

The decision gate should confirm that every POA&M item has complete corrective work; no item is merely waiting for evidence; independent validation is complete; documentation reflects the remediated environment; scope has not changed in a way that invalidates assumptions; provider dependencies are resolved; and the evidence package can be followed by someone outside the implementation team.

The project manager should present unresolved uncertainty explicitly. If one item remains questionable, the decision should focus on resolving it before closeout rather than hoping the formal closeout activity will interpret it favorably. DoD's current FAQ makes this particularly important because a finalized closeout with remaining NOT MET requirements terminates Conditional status.

Deepening Note — Operational Plans of Action After Final Status

Remediation discipline does not stop after Final status. DoD's current FAQ distinguishes Operational Plans of Action from formal CMMC POA&Ms. OPAs can

be used to manage vulnerabilities, patches, temporary deficiencies, and routine maintenance after security requirements have been implemented. They are part of continuous operations rather than a mechanism for carrying an unmet CMMC assessment requirement through Conditional status.

An MSP should therefore maintain an operational corrective-action process even for customers with Final status. New vulnerabilities, failed agents, expired certificates, backup failures, configuration drift, and temporary outages need owners and remediation. The organization should assess whether any new condition affects continuous compliance, scope, contractual reporting, or the basis for annual affirmation.

This distinction strengthens the book's overall message: compliance is not a one-time assessment event. Formal POA&M rules govern a limited post-assessment path; operational remediation is continuous.

Deepening Tool — Closeout Readiness Decision Record

Decision Check	Yes/No	Evidence / Approval Reference
All formal POA&M items technically implemented		
All items independently validated		
No unresolved NOT MET condition known to management		
SSP and supporting documentation reconciled		
Evidence package complete and accessible		
Scope changes reviewed		
Provider dependencies resolved		
CMMC UID and status dates verified		
Internal completion date leaves closeout contingency		
Executive owner authorizes proceeding to formal closeout		

Appendix G
CMMC Assessment Preparation Checklist

Detailed Teaching, Evidence, Interview, Demonstration, and Assessment-Day Readiness Edition

Authored by Dr. Charles Edwards

G.1 Purpose and Philosophy

Assessment preparation is not the process of decorating an evidence folder shortly before an assessor arrives. It is the process of proving that the organization understands its CMMC scope, has implemented the applicable security requirements, operates those requirements consistently, can produce objective evidence, and can explain the environment accurately through documents, interviews, and demonstrations.

For an MSP-supported contractor, preparation also tests responsibility boundaries. The contractor must be able to explain what it owns, what the MSP operates, what specialized providers perform, what evidence each party produces, and how the contractor maintains visibility and accountability. A technically capable MSP cannot compensate for a customer that does not understand its own environment.

G.2 September 2026 Program Context

This edition must be read in the current implementation context. The Department's current CMMC program page states that Phase II implementation, which had been scheduled for November 10, 2026, was suspended on July 13, 2026, while Phase I remains in place. During the pause, the Department states that cybersecurity compliance with NIST SP 800-171 Revision 2 will be enforced through self-assessments and select government-led assessments. Organizations should therefore verify the current implementation phase, current program guidance, and the language of the applicable solicitation or contract before assuming which assessment type applies.

The suspension does not eliminate the underlying obligation to protect CUI under applicable DFARS requirements. It also does not make assessment preparation unnecessary. A contractor that uses the pause as a reason to stop evidence collection, patching, access reviews, logging, incident-response preparation, or SSP maintenance will create a larger readiness problem later.

G.3 Know Which Assessment You Are Preparing For

The first readiness question is not “Are we CMMC ready?” but “What exact assessment or contractual requirement applies to this organization and this environment?” Level 1 self-assessment, Level 2 self-assessment, Level 2 certification assessment, and government-led assessment activities have different contexts. The solicitation, contract, applicable DFARS clauses, current CMMC implementation phase, and the organization's handling of FCI or CUI should be reviewed together.

The readiness coordinator should preserve the source of the requirement: solicitation section, contract clause, task order, prime-contractor flowdown, or other authoritative direction. This prevents a common mistake in which a company prepares for a level based on sales discussions rather than the actual contractual requirement.

G.4 Assessment Is Evidence of an Operating System

The strongest assessment preparation begins months before assessment day. Access reviews occur because the organization needs them, not because an assessor may ask for them. Restore tests are performed because recoverability matters. Logs are monitored because security events matter. Policies describe real operations. Tickets, approvals, configuration records, reports, and recurring reviews are natural outputs of the security program.

When evidence is created only for an assessment, contradictions appear. A policy may say quarterly while the ticket system shows no quarterly activity. The SSP may describe centralized logging while several systems are silent. The assessment preparation process should expose those contradictions internally while there is still time to correct them.

G.5 Examine, Interview, and Test

The Level 2 Assessment Guide describes three assessment methods: examine, interview, and test. Preparation should therefore never be limited to documents. Examine activities review specifications, mechanisms, activities, and records. Interviews evaluate whether personnel understand and perform their responsibilities. Tests exercise mechanisms or activities to determine whether they operate as expected.

A mature readiness program prepares for all three naturally. Documents and evidence must be current; personnel must understand the processes they actually perform; and

technical mechanisms must work when demonstrated. If a requirement can be explained only by a consultant who wrote the policy, the organization is not truly ready.

G.6 The Assessment Readiness Workstreams

Workstream	Primary Question	Typical Outputs
Contract and requirement	What level/status is actually required?	Clause review, solicitation/contract references, CMMC requirement record
Scope	Where do FCI/CUI and security protection functions exist?	Scope narrative, asset inventory, diagrams, data flows, provider list
Implementation	Are requirements actually implemented?	Configurations, procedures, technical records
Evidence	Can implementation and operation be demonstrated?	Evidence index, reports, tickets, exports, approvals
People	Can responsible personnel explain their work?	Interview roster, role mapping, rehearsal notes
Demonstration	Can mechanisms be shown operating?	Demo scripts, test accounts, validation records
Documentation	Do policies and SSP match reality?	Current SSP, policies, procedures, revision history
Provider coordination	Are MSP/ESP responsibilities clear?	CRM/responsibility matrix, service descriptions, evidence commitments
Assessment logistics	Can the assessment proceed without chaos?	Agenda, room/remote plan, access, contacts, contingency plan

G.7 Scope Validation Before Evidence Collection

Evidence collection should not begin with a random list of screenshots. It should begin with scope. The organization should know where CUI is received, created, processed, stored, transmitted, backed up, viewed, administered, and protected. It should identify assets that process CUI, security protection assets, specialized assets where applicable, external service providers, users, administrators, facilities, remote access paths, and data exchanges.

The scope narrative, network diagrams, data-flow diagrams, asset inventory, SSP, and provider register should agree. If a diagram shows a backup service that the SSP never mentions, or the inventory contains an unmanaged server that the data-flow diagram omits, readiness review should stop and reconcile the discrepancy before assessment.

G.8 Asset Inventory Readiness

An assessment-ready asset inventory is more than a hardware list. It should support the organization's scoping decisions. For each relevant asset, the team should

understand function, owner, location, operating system or platform, management method, security tooling, CUI relationship, and applicable asset category.

The readiness team should sample the inventory against reality. Select endpoints, servers, network devices, cloud services, and administrative systems and verify that they exist, are correctly classified, and are managed as documented. Retired assets should not remain active in management tools, and active assets should not be missing from the inventory.

G.9 CUI and FCI Data-Flow Readiness

Personnel should be able to explain how information enters the environment, where it goes, who can access it, how it leaves, and how it is retained or destroyed. This explanation should be consistent with technical controls and contracts.

A data-flow diagram becomes especially important when an MSP or cloud service is involved. If CUI is exchanged through email, secure file transfer, a collaboration platform, an application, or a managed backup service, the organization should know which systems and providers participate and what responsibilities attach to them.

G.10 SSP Readiness

The System Security Plan should describe the system that exists today. Planned future controls, retired products, old network names, inaccurate responsibility assignments, and copied boilerplate undermine credibility. Each requirement narrative should explain implementation in the organization's actual architecture.

The readiness team should compare SSP statements against evidence and demonstrations. If the SSP says MFA protects remote and privileged access, test the relevant paths. If it says logs are reviewed daily, identify the daily review records. If it says backups are tested quarterly, produce the restore-test evidence. The SSP should operate as a map to the evidence rather than a collection of promises.

G.11 Policy and Procedure Readiness

Policies define management expectations; procedures explain how work is performed. Assessment preparation should confirm that both are approved, current, assigned to owners, and consistent with the SSP and actual operations.

The team should look for policy statements that create obligations no one performs. Overly ambitious language such as “all logs are reviewed continuously” can create an

unnecessary contradiction when the real operating model is risk-based automated monitoring with defined analyst review. Accurate language is more valuable than impressive language.

G.12 Evidence Architecture

Evidence should be organized so a reviewer can move from requirement to implementation to proof. A useful evidence index identifies the requirement, artifact, owner, source system, date or period, evidence location, and what the artifact demonstrates.

The organization should preserve provenance. Screenshots should have enough context to identify the system and setting. Exports should retain meaningful names and dates. Tickets should show chronology and approval. Reports should identify the covered population and time period. Evidence should not depend on unexplained filenames or the memory of one employee.

G.13 Evidence Freshness

Some evidence describes design and changes infrequently; other evidence proves recurring operation. A policy approved last year may still be current, while an access review from eighteen months ago cannot demonstrate a quarterly process operating today. Readiness review should classify evidence by expected freshness.

Recurring evidence commonly includes access reviews, vulnerability scans, patch reports, backup tests, incident exercises, log-review or monitoring records, account changes, training, configuration reviews, and change records. The evidence calendar should ensure that expected cycles continue through assessment preparation.

G.14 Interview Preparation

Interview preparation is not memorizing scripted answers. Personnel should understand their own responsibilities and be able to describe what they actually do. The readiness coordinator should map likely interview topics to the people who perform the work: system owners, administrators, help-desk personnel, security staff, HR, management, incident responders, backup operators, and MSP personnel where applicable.

A rehearsal should identify confusion, not teach people to conceal it. If two administrators describe different account-termination processes, the organization has discovered an operational inconsistency that should be resolved before assessment.

G.15 Demonstration Preparation

Technical demonstrations should be rehearsed because ordinary operational friction can consume assessment time. The organization should know which console, account, device, report, or workflow will demonstrate a mechanism. Access should be tested in advance, especially for remote assessment sessions.

A demonstration should show the actual production or applicable assessed environment, subject to appropriate security controls. Teams should avoid creating a special assessment-only configuration that is not representative of normal operation.

G.16 Evidence Versus Demonstration

Evidence and demonstration answer different questions. A current configuration export may show how a system is configured. A live demonstration can show how an administrator performs the process or how the mechanism responds. Historical records can show that the process operated over time.

The strongest readiness package combines these perspectives. For example, MFA readiness may include identity policy configuration, a live sign-in demonstration, authentication logs, exception records, and privileged-account review evidence.

G.17 MSP and Customer Interview Boundaries

The contractor should not outsource every interview to the MSP. The MSP can explain systems it operates, but contractor personnel should understand business processes, scope, approvals, risk decisions, information flows, and oversight.

Likewise, MSP personnel should not speculate about customer decisions they do not own. A clear responsibility matrix allows each party to answer within its role and hand off appropriately when another party owns the subject.

G.18 Provider Evidence Readiness

If a security requirement depends on an external service provider, evidence should not first be requested the week before assessment. Contracts and service descriptions

should define evidence availability, responsible contacts, retention, and response time.

The readiness team should test provider evidence retrieval in advance. Can the SOC produce the requested log-health report? Can the backup provider show restore evidence? Can the MSP provide named administrator records? Can the cloud service configuration be demonstrated? If the answer depends on opening a vendor case with an unknown response time, that is an assessment risk.

G.19 Identity and Access Readiness

Identity readiness should cover user lifecycle, privileged identities, MFA, remote access, service accounts, inactive accounts, shared-account restrictions, authorization, and recurring review. Evidence should connect policy to actual identities.

The team should sample joiners, movers, and leavers. It should test that terminated users are disabled, role changes are reflected, privileged access is limited, and exceptions are documented. MSP technician accounts require the same scrutiny because they may have broad access to the assessed environment.

G.20 Endpoint Readiness

Endpoints should be reconciled across inventory, management, EDR, vulnerability, encryption, and patching systems. A laptop appearing in inventory but not in EDR or MDM should be investigated. A security agent installed but unhealthy is not equivalent to an operating control.

Readiness sampling should include ordinary user endpoints, privileged administration devices where applicable, remote devices, and systems with unusual business functions. The team should understand how new devices are enrolled and how missing agents or configuration drift are detected.

G.21 Vulnerability and Patch Readiness

The organization should be able to demonstrate discovery, prioritization, remediation, exception handling, rescanning, and closure. A vulnerability report alone proves discovery, not management.

Select several vulnerabilities from different periods and trace them end to end: scan finding, ticket, owner, corrective action, change record, rescan, and closure. Overdue

vulnerabilities should have documented management treatment rather than disappearing from reports.

G.22 Logging, SIEM, and SOC Readiness

Assessment preparation should verify that required log sources are actually reporting, not merely configured to report. The team should understand retention, alerting, analyst workflow, escalation, time synchronization, and log-source health monitoring.

A useful rehearsal deliberately traces one event from source system to collection platform to detection or analyst review. The organization should also be prepared to explain what happens when a critical source stops sending logs.

G.23 Backup and Recovery Readiness

Successful backup jobs are not enough. The organization should demonstrate that protected data can be restored and that recovery access, encryption keys, retention, and responsibilities are understood.

Restore-test evidence should show what was restored, from which recovery point, where it was restored, who validated it, and whether integrity and permissions were checked. Provider-managed backup does not eliminate the contractor's need to understand recovery.

G.24 Configuration and Change Management Readiness

The readiness team should select representative changes and trace approval, implementation, testing, and documentation. Baselines should be current and deviations understood.

Emergency changes deserve attention because they often bypass normal documentation. The organization should show how emergency work is retrospectively reviewed and how configuration drift is detected.

G.25 Incident Response Readiness

Personnel should know how to recognize, report, escalate, contain, investigate, and document an incident. The incident-response plan should identify roles, contacts, provider responsibilities, decision authority, and applicable contractual reporting paths.

Tabletop exercises should test realistic scenarios involving CUI, compromised credentials, ransomware, lost devices, or provider incidents. Exercise findings should produce corrective actions rather than a ceremonial attendance sheet.

G.26 Physical and Personnel Readiness

Assessment preparation should not focus only on cloud and endpoint technology. Physical access, visitor controls, media handling, personnel screening where applicable, termination, training, and facility practices must match documented procedures.

Remote and hybrid work should be included. Personnel should understand rules for home workspaces, printing, removable media, device storage, and remote access where those activities are allowed.

G.27 Evidence Room Design

A well-designed evidence repository reduces assessment friction. Organize evidence by requirement or a controlled cross-reference structure, maintain an index, use consistent filenames, preserve versions, and restrict access appropriately.

Do not create uncontrolled duplicate evidence sets on desktops, email threads, and shared drives. The readiness coordinator should know which repository is authoritative.

G.28 Assessment-Day Roles

Assessment day should have defined roles: executive sponsor, assessment coordinator, evidence coordinator, technical leads, interview participants, MSP liaison, and documentation support. One person should manage requests so multiple teams do not produce conflicting evidence.

The coordinator should track every assessor request, responsible owner, status, artifact supplied, and follow-up. This request log becomes essential during a multi-day assessment.

G.29 Remote Assessment Logistics

For remote activity, verify conferencing, screen sharing, authentication, secure evidence exchange, participant availability, time zones, and backup communication

methods. Test privileged-console access from the location where the demonstration will occur.

Sensitive evidence should not be sent through improvised channels simply because the assessment is remote. The evidence-handling method should be agreed and controlled.

G.30 What Not to Do During an Assessment

Personnel should not guess. If a participant does not know an answer, the coordinator should identify the appropriate owner or evidence rather than inventing an explanation. Teams should not alter configurations during a demonstration merely to produce the expected result without transparently addressing the condition.

The organization should also avoid flooding assessors with irrelevant material. More evidence is not automatically better evidence. The objective is to provide sufficient, relevant, traceable evidence for the requirement being evaluated.

G.31 90-Day Assessment Preparation Model

Period	Primary Focus	Expected Outcome
Days 90–76	Confirm requirement, scope, SSP, asset inventory, providers	Authoritative assessment boundary and readiness plan
Days 75–61	Requirement-by-requirement internal review	Known gaps and evidence deficiencies identified
Days 60–46	Remediation and evidence-cycle completion	Material weaknesses corrected; recurring evidence current
Days 45–31	Interview and demonstration rehearsals	Personnel and systems ready to explain/show operation
Days 30–16	Independent readiness review	Contradictions, missing evidence, and weak demonstrations corrected
Days 15–8	Evidence freeze/index quality review	Authoritative evidence set organized and accessible
Days 7–1	Logistics, participant availability, final delta checks	Assessment can begin without operational confusion
Assessment period	Controlled response, evidence tracking, demonstrations	Accurate, traceable assessment support

G.32 Party ABC — Existing Contractor

Party ABC already handles CUI and uses Party IJK as its MSP. Ninety days before a planned assessment, ABC validates its CUI flows and discovers that one engineering application and a managed backup service were not clearly represented in the SSP. Instead of beginning with evidence collection, ABC corrects scope documentation and the responsibility matrix.

ABC then performs requirement-by-requirement readiness review. IJK supplies technical evidence for identity, endpoints, logging, vulnerability management, backup, and network controls. ABC supplies policies, approvals, business-process evidence, training, HR lifecycle records, and management oversight. Interview rehearsals reveal that ABC and IJK use different terminology for incident escalation, so the procedure and service workflow are reconciled before assessment.

G.33 Party EGH — Prospective Offeror

Party EGH is preparing before receiving CUI. It uses the assessment checklist as a build-validation tool. Rather than waiting for a formal assessment date, EGH requires every implemented requirement to have an owner, evidence source, demonstration method, and SSP narrative.

This approach exposes planned-but-not-operating controls early. A backup service may be purchased but not restore-tested; MFA may be licensed but not applied to every administrative path; logging may be configured but lack health monitoring. EGH corrects these conditions before treating the environment as assessment ready.

G.34 Party IJK — MSP Supporting Multiple Assessments

Party IJK maintains a reusable evidence capability but never assumes one customer's evidence automatically applies to another. Shared MSP processes may support multiple customers, but customer-specific configurations, identities, assets, scope, contracts, and evidence remain separated.

IJK designates an assessment liaison for each customer, validates technician availability, tests evidence retrieval, and maintains a provider-side responsibility map. When a customer asks IJK to answer a question outside its responsibility, the liaison redirects the question to the appropriate customer owner rather than speculating.

G.35 Master Pre-Assessment Checklist

- Current solicitation/contract/flowdown and required CMMC level verified.
- Current CMMC implementation phase and applicable DoD guidance rechecked.
- Scope narrative approved and consistent with SSP.
- CUI/FCI flows validated.
- Asset inventory reconciled to technical management systems.
- External service providers identified and documented.
- Responsibility matrix current.

- SSP reflects the operating environment.
- Policies and procedures are current, approved, and practiced.
- Every applicable requirement has an implementation owner.
- Every applicable requirement has mapped evidence.
- Recurring evidence is current.
- Known gaps have been remediated or appropriately governed.
- Identity lifecycle and privileged access sampled.
- Endpoints reconciled across inventory, EDR, MDM, vulnerability, encryption, and patch tools.
- Vulnerability findings traced through remediation and rescan.
- Critical log sources and SIEM health validated.
- Backup restoration demonstrated.
- Configuration/change records sampled.
- Incident-response exercise completed and corrective actions tracked.
- Physical/personnel processes reviewed.
- Interview roster prepared.
- Interview rehearsals completed without scripted memorization.
- Technical demonstrations rehearsed.
- Provider evidence retrieval tested.
- Evidence repository indexed and access-controlled.
- Assessment request log prepared.
- Assessment-day roles assigned.
- Remote/on-site logistics tested.
- Executive sponsor understands scope, status, and unresolved risks.

G.36 Evidence Index Template

Req./Objective	Artifact	Owner	Source System	Period/Date	What It Demonstrates	Repository Ref.	Validated By

G.37 Interview Readiness Matrix

Role	Topics	Processes Performed	Evidence They Can Explain	Backup Interviewee	Rehearsal Status
Executive sponsor					
Security/compliance lead					
System administrator					
Help desk / identity admin					
Incident responder					
MSP technical lead					

G.38 Demonstration Readiness Matrix

Requirement/Topic	System/Console	Demo Owner	Account Needed	Expected Demonstration	Fallback Evidence	Tested Date
MFA / identity						
Endpoint security						
Vulnerability management						
Logging / SIEM						
Backup restore						
Change management						

G.39 Assessment Request Log

Request #	Date/Time	Assessor Request	Requirement	Owner	Evidence/Demo Supplied	Status	Follow-Up

G.40 Final Readiness Decision Gate

The final readiness decision should be made by management using evidence, not optimism. The organization should ask whether scope is stable, documentation matches reality, technical mechanisms operate, recurring processes have current records, interview participants understand their roles, demonstrations work, provider evidence is accessible, and known weaknesses have been resolved or handled under the applicable rules.

If the answer depends on last-minute configuration changes, untested evidence, unavailable providers, or planned future implementation, the organization should treat that as readiness risk. A successful assessment should be the natural consequence of a functioning security program, not a performance created for assessment week.

G.41 Regulatory and Source Verification Note

This September 2026 teaching edition was verified against the Department's current CMMC program materials, the CMMC Level 2 Assessment Guide, 32 CFR part 170 references identified by the Department, and the November 2025 version of DFARS 252.204-7021. The current program page states that Phase II implementation was suspended on July 13, 2026 and that Phase I remains in place. The Level 2 Assessment Guide remains an official preparation and assessment reference and describes assessment objectives and the examine, interview, and test methods. DFARS 252.204-7021 establishes requirements concerning current CMMC status, CMMC UIDs, annual affirmations of continuous compliance, SPRS, flowdown, and successful POA&M closeout when a contractor has Conditional status. Because the program is actively under review, readers must verify the current CMMC program guidance, 32 CFR part 170, applicable DFARS clauses, and the specific solicitation, contract, task order, or flowdown before making a contractual or assessment decision.

Deepening G.5 — Preparing for Examine, Interview, and Test

The official Level 2 Assessment Guide organizes each security requirement around assessment objectives and identifies potential assessment methods and objects. The three methods—examine, interview, and test—should shape the entire readiness program. An organization should not assume that one strong document compensates for a weak interview or a failed technical demonstration.

For examine preparation, the readiness team should ask what specifications, mechanisms, activities, and records establish that each assessment objective is satisfied. This may include SSP narratives, policies, procedures, configuration exports, system reports, tickets, access reviews, diagrams, training records, incident records, scan results, and change documentation. Each artifact should have a clear purpose. The evidence index should state what objective the artifact supports rather than simply listing a filename.

For interview preparation, the team should identify the individual who actually performs or owns the activity. A system administrator should be able to explain privileged-account provisioning; HR and IT may jointly explain termination; the SOC analyst can explain alert triage; the system owner can explain business authorization. Interviewees should speak from experience, not recite a consultant's wording.

For test preparation, the team should know what mechanism can be exercised and what result should be observable. If testing account lockout, the organization should understand the configuration and safe demonstration method. If demonstrating logging, it should trace an event from source to collection and review. A rehearsal should confirm that the demonstration works without changing the environment merely for assessment day.

Deepening G.7 — Scope Validation as the First Assessment Control

Scope errors contaminate everything that follows. If an asset or provider is omitted from scope, the evidence package may be complete for the wrong environment. The readiness team should therefore perform a scope walk before requirement-by-requirement evidence review.

Start with information rather than technology. Select representative CUI transactions and trace them from receipt or creation through processing, storage, transmission, collaboration, backup, administration, and disposition. At each step identify the user, device, application, network path, cloud service, security service, and external provider involved. Then compare that observed path with the SSP, diagrams, asset inventory, and provider register.

The team should deliberately search for shadow paths: email forwarding, local downloads, temporary file shares, unmanaged printers, mobile access, remote support, vendor portals, backup replicas, administrator workstations, and troubleshooting exports. These are often where the documented boundary diverges from actual operations.

For MSP-supported environments, the scope walk should also identify systems that provide security protection. An RMM platform, SIEM, EDR management console, identity service, vulnerability platform, backup service, or remote administration tool may play an important security role even when it is not the primary business system holding CUI. The current Level 2 Scoping Guide and applicable provider treatment should be consulted when classifying these relationships.

Deepening G.10 — Turning the SSP Into an Assessment Roadmap

A useful SSP lets an assessor and the organization's own readiness team understand the system without reverse-engineering it from scattered evidence. Each implementation narrative should answer who performs the activity, what technology or process is used, where it applies, how often it occurs when recurring, what exceptions exist, and where supporting evidence can be found.

Readiness review should perform a two-way trace. First, start with the SSP statement and locate technical or procedural evidence proving it. Second, start with the actual system and confirm that the SSP accurately describes it. The second direction catches undocumented technology and provider changes.

Planned language deserves special scrutiny. Statements such as “will implement,” “is being deployed,” or “planned for Q4” may reveal that the requirement is not operating. The SSP should not disguise future work as current implementation. Where a requirement is satisfied through several mechanisms, the narrative should explain how they work together rather than naming products without describing their function.

Deepening G.12 — Evidence Sufficiency, Relevance, and Provenance

Assessment evidence should be sufficient to support the assessment objective, relevant to the assessed environment, and traceable to an authoritative source. The readiness team should challenge every artifact with three questions: What exactly does this prove? Does it apply to the correct population and time period? Can another reviewer understand where it came from?

A screenshot of an MFA policy may demonstrate configuration but not necessarily that every required account is covered. A user list can help establish population but not prove authentication behavior. Sign-in records may demonstrate operation but must be connected to the correct identities and period. Strong evidence often comes from combining artifacts rather than searching for one perfect screenshot.

Provenance matters because evidence without context is fragile. Filenames should identify the system, purpose, and date. Exports should preserve metadata where practical. Screenshots should show enough surrounding context to identify the console and setting without exposing unnecessary sensitive data. Manually created summaries should reference the source records from which they were derived.

The evidence coordinator should also identify contradictory evidence. If one report shows 142 managed endpoints and another shows 139 EDR sensors, the discrepancy should be investigated rather than hidden. The assessment preparation process should explain legitimate differences or correct missing coverage.

Deepening G.13 — Evidence Freshness and Recurring Operations

Readiness is stronger when evidence demonstrates repeated operation rather than a single assessment-week event. For recurring activities, the organization should preserve a sequence showing that the process operated over time. A quarterly access review should have multiple cycles when the system has been operating long enough; vulnerability management should show discovery, remediation, and rescanning across several periods; backup testing should show recurring recovery validation.

The evidence calendar should identify each recurring activity, frequency, owner, expected artifact, repository, and next due date. This calendar becomes an operational management tool, not merely an assessment checklist.

A late or missed cycle should not be concealed. The readiness team should determine why it was missed, correct the process, document remediation, and assess whether the gap affects the organization's claim that the requirement is implemented. Evidence integrity is more important than manufacturing a perfect-looking history.

Deepening G.14 — Interview Rehearsal Without Coaching Answers

The purpose of an interview rehearsal is to determine whether the organization operates consistently. The facilitator should ask open questions such as, “Walk me through what happens when an employee leaves,” “How do you know a new laptop has all required security agents?” or “What happens when a critical log source stops reporting?” These questions reveal whether personnel understand the workflow.

The facilitator should then compare answers across roles. HR may say termination notices are sent immediately, while the help desk may say accounts are disabled only

after a manager submits a ticket. That difference is a readiness finding. The correct response is to reconcile the process, not teach both people to repeat identical wording.

Interviewees should understand when to say that another role owns part of the answer. An MSP engineer can explain EDR deployment but may not know why the contractor authorized a particular user. The contractor's manager can explain authorization but may not know the sensor's deployment mechanics. A mature interview shows coordinated responsibilities rather than one person pretending to know everything.

Deepening G.15 — Technical Demonstration Engineering

Every planned demonstration should have a short internal runbook. The runbook identifies the requirement or objective, system, production-safe demonstration steps, expected result, person driving the console, person explaining the process, required account, evidence fallback, and any safety constraints.

The team should test authentication and permissions before assessment day. A demonstration can fail for mundane reasons: an administrator's password expired, a browser blocks a government-cloud endpoint, a VPN route is unavailable from the conference room, or the designated engineer lacks access to a report. These failures do not necessarily mean the security mechanism is deficient, but they consume time and create uncertainty.

The readiness team should also distinguish a live test from a guided display. Showing a configuration page is not the same as exercising the mechanism. Where the assessment method calls for testing, preparation should identify a safe way to demonstrate behavior without disrupting production.

Deepening G.18 — ESP and MSP Evidence Packages

Provider evidence should be designed around responsibility. For each security requirement that depends partly on Party IJK or another ESP, the responsibility matrix should identify what the contractor implements, what the provider implements, who operates the mechanism, who generates evidence, and who can demonstrate it.

The provider evidence package should include service descriptions, relevant responsibility mappings, customer-specific configuration evidence, named administrative access records, operational reports, incident/escalation workflow

evidence, and applicable technical demonstrations. Generic marketing material is not a substitute for evidence of the customer's configured service.

The customer should test the provider evidence path months before assessment. If evidence requires a special report from the SOC, request one during readiness. If an MSP administrator must join the assessment, schedule a rehearsal. If the provider cannot produce evidence needed to support the claimed implementation, the issue is a readiness gap that should be resolved before assessment.

Deepening G.19 — Identity and Privileged Access Assessment Walkthrough

A mock assessor should begin with the identity population. How are users created? Who authorizes access? What distinguishes standard and privileged identities? How are service accounts governed? What happens to dormant accounts? How are remote and privileged paths protected?

The team should select several identities and trace them through their lifecycle. For a new employee, examine authorization, provisioning, group membership, MFA enrollment, and device access. For a transferred employee, verify that old access was removed and new access approved. For a terminated employee, verify timing and completeness of disablement. For an administrator, examine named privileged credentials, role assignment, authentication, and review records.

The MSP's identities should be included where they access the environment. Shared technician accounts, stale vendor accounts, emergency credentials, and unmanaged service identities are common areas requiring careful explanation and evidence.

Deepening G.20 — Endpoint Population Reconciliation

Endpoint readiness should use population reconciliation rather than isolated screenshots. Export the authoritative asset list and compare it with MDM/RMM enrollment, EDR health, vulnerability coverage, encryption status, and patch-management populations. Differences should be categorized and resolved.

Some differences may be legitimate: a network appliance will not appear in an endpoint EDR console, and a decommissioned device may remain in historical reports. The readiness record should explain these differences. Unexplained gaps are more concerning than differences themselves.

The team should sample endpoint build and retirement workflows. A new system should automatically or reliably receive the required configuration and security agents. A retired system should be removed from active access and management populations. This demonstrates that endpoint security is a lifecycle process rather than a one-time deployment.

Deepening G.21 — Vulnerability Evidence From Discovery Through Closure

Select actual findings and follow their complete history. The initial scan establishes discovery. The ticket or remediation record establishes ownership. The change record shows implementation. The rescan or equivalent verification establishes that the condition is resolved. Exceptions should show approval, rationale, compensating operational treatment where applicable, expiration, and continued tracking.

Readiness teams should examine aging. A report containing many old critical or high-impact findings may reveal that scanning exists but remediation governance is weak. Management should understand why items remain open and whether the remediation process operates according to documented expectations.

The team should also validate scan coverage. A clean report is not meaningful if important assets are absent from the scanner population or authenticated scanning is failing.

Deepening G.22 — SIEM and SOC Assessment Walkthrough

Start with the expected log-source inventory. Compare expected sources with actual ingestion. Confirm timestamps, source identity, retention, health monitoring, alerting, and analyst workflow. The organization should know how it detects a silent source.

Then trace a representative security event. Generate or identify a safe event at the source, locate it in the logging platform, show the relevant parsing or fields, demonstrate how the event becomes visible to the analyst, and explain escalation. Historical tickets can show that the workflow operates outside the demonstration.

For an outsourced SOC, divide the explanation clearly. The MSP or MSSP may operate collection and triage, while the contractor decides business impact, containment authority, contractual reporting, or user actions. The evidence should demonstrate the handoff.

Deepening G.23 — Backup and Recovery Assessment Walkthrough

The readiness team should identify what is protected, backup frequency, retention, repository, encryption, administrative access, monitoring, and restoration responsibilities. Then select a completed restore test and trace it from request to recovered data.

A strong restore record identifies the recovery point, target location, data restored, elapsed time where relevant, integrity validation, permissions validation, errors encountered, and person accepting the result. A screenshot showing “job successful” demonstrates backup execution but not recoverability.

Where the MSP operates backup, the contractor should still know recovery priorities, authorization, and how to request restoration. Provider operation does not remove customer governance.

Deepening G.25 — Incident Response Interview and Tabletop Readiness

An incident-response rehearsal should test decision-making, not merely whether personnel know a phone number. Present a realistic scenario: a user reports a suspicious login followed by unusual file activity in a CUI environment. Ask who receives the report, who validates the event, who can disable the account, who isolates the endpoint, who preserves evidence, who contacts management, and who evaluates contractual reporting obligations.

Then introduce complications. The affected user is an executive. The endpoint is remote. The MSP detects the event before the customer. A cloud provider is involved. The exercise should reveal authority gaps and handoff problems.

After the exercise, corrective actions should be tracked like any other remediation. Assessment readiness improves when the organization can show that exercises lead to process improvements.

Deepening G.27 — Evidence Room Architecture and Request Discipline

The evidence repository should support controlled retrieval without allowing uncontrolled browsing of unrelated sensitive material. A master index can map each requirement/objective to evidence references while permissions limit who can access source artifacts.

During assessment, the evidence coordinator should record what was requested, what was supplied, when it was supplied, and whether follow-up is pending. This prevents duplicate or contradictory submissions. If an updated artifact replaces an earlier one, the request log should record the replacement.

The organization should avoid giving assessors an uncurated dump of entire administrative repositories when a specific relevant artifact can answer the request. Evidence handling should be responsive while still protecting information unrelated to the assessment.

Deepening G.28 — Assessment-Day Command Structure

The assessment coordinator manages flow rather than answering every question. Technical questions go to technical owners; business authorization questions go to contractor management; provider-operation questions go to the MSP or ESP; evidence requests go through the evidence coordinator.

A short internal meeting at the beginning and end of each assessment day can review scheduled activities, open requests, unresolved questions, next-day participants, and evidence quality. The team should distinguish a request for clarification from a newly discovered technical problem.

If a genuine weakness is discovered during assessment, the organization should handle it transparently under the applicable assessment process. Quietly changing a configuration while implying it was always configured that way creates both credibility and evidence-integrity problems.

Deepening G.31 — Using the 90-Day Model as a Gated Program

The 90-day model should use decision gates rather than merely dates. At the scope gate, the organization confirms the boundary and provider relationships. At the implementation gate, it confirms that known material gaps have corrective plans and credible completion dates. At the evidence gate, it confirms that each objective has sufficient support. At the rehearsal gate, interviews and demonstrations operate successfully. At the final readiness gate, management decides whether the organization is genuinely prepared.

A failed gate should trigger remediation, not optimistic advancement to the next phase. For example, if scope remains unstable at day 60, the team should not spend most of its effort polishing evidence for a boundary that may change.

The schedule should also preserve normal security operations. Assessment preparation should not consume so much staff time that patching, monitoring, access reviews, or incident response deteriorate.

Deepening G.32 — Party ABC Full Mock-Assessment Scenario

Party ABC conducts a three-day internal mock assessment with a reviewer who did not build the environment. Day one focuses on scope, SSP, identity, and access control. The reviewer traces two CUI workflows and discovers that an engineering export is temporarily stored in a location absent from the data-flow diagram. ABC records a scope/documentation finding rather than explaining it away.

Day two focuses on endpoint, vulnerability, logging, configuration, and backup operations. Population reconciliation finds 146 active endpoints, 146 in RMM, 145 in EDR, and 144 in the vulnerability platform. Investigation shows one EDR sensor is unhealthy and two newly deployed systems missed vulnerability enrollment. Party IJK corrects the provisioning workflow and validates the full population.

Day three focuses on incident response, personnel processes, evidence quality, and provider handoffs. An interview reveals that ABC's incident plan tells employees to contact the security manager, while IJK's service procedure tells users to call the help desk. ABC and IJK reconcile the workflow and conduct a tabletop using the corrected process.

The mock assessment succeeds because it discovers weaknesses. ABC does not grade the exercise by how few findings appear. It grades the exercise by whether it exposes conditions that would otherwise appear during the formal assessment and whether those conditions are corrected with evidence.

Deepening G.40 — The Final Readiness Decision

Management should receive a concise readiness package: confirmed assessment requirement, scope statement, unresolved-risk summary, requirement/objective readiness status, evidence-completeness status, interview rehearsal results, demonstration results, provider readiness, and logistics status.

The decision should distinguish “documentation complete” from “implementation demonstrated.” A requirement should not be considered ready merely because an evidence folder exists. Conversely, a working technical control with no durable evidence may still create assessment difficulty.

The executive sponsor should ask one final question: if the assessment began tomorrow and the assessor selected any applicable objective, could the organization identify the responsible person, explain the implementation, produce relevant evidence, and demonstrate the mechanism where appropriate without changing the environment first? That is a more meaningful readiness test than a percentage-complete dashboard.

Substantive Depth Pass — Requirement-by-Requirement Readiness Method

The final substantive readiness pass should be conducted at the assessment-objective level rather than at the broad control-family level. For every applicable Level 2 security requirement, the readiness team should identify the individual assessment objectives in the current Level 2 Assessment Guide and determine how each objective will be supported through examine, interview, test, or an appropriate combination. This prevents a common mistake in which a team concludes that a requirement is ready because one attractive artifact exists even though another portion of the requirement has not been demonstrated.

For each objective, the team should record the implementation narrative, responsible organization, operational owner, evidence source, interview participant, demonstration mechanism, evidence period, and validation result. The reviewer should then challenge the package as an assessor would: does the evidence actually address the objective, does it represent the assessed environment, and does it demonstrate implementation rather than intention?

The organization should not create its own substitute assessment criteria. The official assessment guide remains the reference for the objectives and methods. The internal matrix is a management mechanism that helps the organization prepare systematically for those official objectives.

Substantive Depth Pass — The Objective Readiness Record

A useful Objective Readiness Record contains enough information that a reviewer who did not build the control can evaluate preparation. The record begins with the applicable security requirement and assessment objective. It then identifies the systems and populations affected, the SSP section describing implementation, and the parties responsible for implementation and operation.

Next, the record identifies examine artifacts. These may include policies, procedures, diagrams, configuration exports, tickets, reports, approvals, inventories, logs, or recurring review records. It identifies interview participants based on actual responsibility and defines a production-safe demonstration where testing is appropriate.

Finally, the record captures the internal validation conclusion and unresolved questions. The conclusion should not merely say “ready.” It should explain why the objective is supported and identify the evidence that led to that conclusion. This creates traceability between readiness work and the formal assessment methodology.

Substantive Depth Pass — Evidence Triangulation

One of the strongest preparation techniques is evidence triangulation: confirming the same implementation through different evidence perspectives. A policy states what should happen. A configuration shows how a mechanism is established. A historical record shows that the process actually operated. An interview explains how personnel perform the work. A test demonstrates behavior.

Consider account termination. The policy may require prompt disablement. The HR record establishes the termination event. The service ticket establishes notification and workflow. The identity-system record establishes disablement. An interview explains responsibility. Sampling several terminated users demonstrates that the process operates repeatedly. Together, these artifacts are stronger than any one artifact in isolation.

Triangulation also exposes contradictions. If the procedure says the help desk disables accounts but the actual tickets show the MSP performs the action, the documentation should be corrected. If the policy requires quarterly review but only one annual review exists, the process itself may require remediation.

Substantive Depth Pass — Sampling Strategy for Internal Mock Assessments

A mock assessment should use sampling intelligently. The goal is not to inspect every asset and transaction; it is to select enough representative examples to expose weaknesses in the process. Sampling should include ordinary and difficult cases: standard users and privileged users, current employees and terminated employees, normal endpoints and specialized systems, recent vulnerabilities and aged findings, routine changes and emergency changes.

The readiness reviewer should avoid allowing process owners to select only their cleanest examples. A stronger method is to obtain the relevant population and select samples independently. If the organization claims that all endpoints receive EDR, the reviewer should compare populations rather than ask for a screenshot of one protected laptop.

Where a sample exposes a defect, the team should determine whether the defect is isolated or systemic. One missing agent may represent a device-specific failure, or it may reveal a provisioning workflow that allows systems to bypass enrollment. Root-cause analysis determines the difference.

Substantive Depth Pass — Full Mock Assessment Evidence Package

The mock assessment package should resemble the structure needed for a real assessment without pretending to be an official assessment. It should contain the confirmed scope, current SSP, asset and provider inventories, responsibility matrix, objective readiness matrix, evidence index, interview roster, demonstration matrix, open-finding register, request log, and management readiness decision.

Each artifact should have version control. The evidence index should identify which artifacts are authoritative and which are supporting references. Where one artifact supports several objectives, the index should cross-reference it rather than create uncontrolled copies.

At the end of the mock assessment, the reviewer should issue findings in language that describes the observed condition, affected population, expected requirement or process, supporting evidence, and remediation owner. The purpose is to drive correction, not to imitate the authority of a C3PAO.

Substantive Depth Pass — Evidence Package Example: Privileged Access

Assume Party ABC uses named administrative accounts for server administration and Party IJK performs much of the technical work. The readiness package begins with ABC's policy and SSP description of privileged access. The identity export identifies privileged groups and members. Approval records show why each administrator received access. MFA configuration and authentication records show how privileged access is protected. Quarterly access-review records demonstrate recurring governance.

The interview component includes ABC's system owner, who explains authorization and oversight, and IJK's technical lead, who explains provisioning and administration. The demonstration uses a designated administrative account to show authentication and access to an approved management function. The reviewer then samples a former technician to verify that privileged access was removed.

If a generic shared administrator account still exists for a legacy device, the team must understand its purpose, protection, use, monitoring, and remediation status rather than omitting it from the package.

Substantive Depth Pass — Evidence Package Example: Vulnerability Management

The vulnerability-management package should establish scope, scanning operation, finding management, remediation, verification, and governance. Start with the asset population and scanner coverage. Show the scanning configuration and a current authenticated scan where applicable. Select several findings and trace them through tickets, assignment, change implementation, rescanning, and closure.

Include an aged finding. The purpose is not to showcase failure but to demonstrate governance. The organization should be able to explain why the finding remains open, what actions have occurred, who owns the decision, and how the condition continues to be tracked.

Interview the person who reviews results and the person who performs remediation. Demonstrate how a new finding becomes a managed work item. The evidence should show an operating lifecycle rather than a monthly PDF report that no one acts upon.

Substantive Depth Pass — Evidence Package Example: Security Logging

The logging package should connect the source population to actual ingestion. Begin with the documented list of expected critical sources. Compare it with the SIEM or logging platform. Select a representative server, identity platform, firewall, endpoint security source, and other relevant systems and confirm that events are arriving.

Then demonstrate operational monitoring. Trace an event into the platform, show the relevant detection or review process, and connect it to a historical alert or ticket. Show how the SOC or responsible team detects a source that stops reporting.

For Party IJK, the evidence must distinguish provider operation from Party ABC's responsibilities. IJK may monitor and escalate; ABC may own business decisions, containment authority, and contractual reporting. The assessment preparation package should make that handoff visible.

Substantive Depth Pass — Evidence Package Example: Backup and Recovery

The backup package should begin with the protected-data and system inventory. It should identify backup frequency, retention, storage location, access restrictions, encryption, monitoring, and recovery responsibilities. A current job-success report is useful but insufficient by itself.

Select a completed restore test. The record should show the recovery point, restored content, target location, authorization, recovery steps, validation of integrity, validation of access permissions, problems encountered, and acceptance. Interview both the provider operator and the contractor owner where responsibilities are divided.

The readiness reviewer should ask what happens if the primary backup administrator is unavailable, credentials are compromised, or an encryption key becomes inaccessible. These questions test whether recovery is an operational capability rather than a product subscription.

Substantive Depth Pass — Managing Findings During the Mock Assessment

All mock-assessment findings should enter a controlled remediation register. Each finding should contain the observed condition, affected assets or process, requirement/objective relationship, root cause, corrective action, owner, milestones, evidence required for closure, target date, and independent validation result.

The team should distinguish documentation findings from implementation findings, but it should not assume documentation findings are trivial. An inaccurate SSP can obscure scope or responsibility. Likewise, a technical configuration issue may reveal a broader process defect.

Closure should require evidence. The person who performed the correction should not be the only person deciding that the finding is closed. An independent reviewer

should verify that the corrective action addresses the root cause and that the supporting evidence is complete.

Substantive Depth Pass — Interview Question Bank by Role

Executive leaders should be prepared to explain governance, responsibility, resources, risk decisions, and how they know the security program operates. System owners should explain authorization, information flows, system purpose, and oversight. Administrators should explain configuration, account management, patching, logging, and change procedures. Help-desk personnel should explain identity verification, ticket workflows, escalation, and user lifecycle events.

Security personnel should explain monitoring, vulnerability management, incident handling, evidence retention, and escalation. HR personnel should explain onboarding, transfers, termination, and coordination with IT. MSP personnel should explain only the services and mechanisms they actually operate.

Questions should be conversational and operational: “Show me how you know,” “What happens next?” “Who approves that?” “What happens if the normal process fails?” and “Where is the record?” These questions are more effective than asking personnel to recite control numbers.

Substantive Depth Pass — Demonstration Failure and Recovery Protocol

A rehearsal should establish what to do when a demonstration does not behave as expected. First, do not improvise configuration changes. Determine whether the problem is a demonstration-access issue, a temporary operational issue, or evidence of a control weakness. Record what happened.

If a report will not load but historical evidence and configuration remain available, the team may use appropriate supporting evidence while troubleshooting. If the mechanism itself fails, the condition should be treated as a substantive finding and handled transparently.

This protocol protects evidence integrity. Assessment pressure should never cause personnel to alter the environment silently simply to make a screen look correct.

Substantive Depth Pass — Provider Coordination Conference

Thirty to forty-five days before an assessment, the contractor should conduct a formal provider coordination conference with the MSP, MSSP, CSP, backup provider, and other material providers as applicable. The meeting should review scope, responsibility, interview participation, demonstration ownership, evidence retrieval, escalation contacts, availability, and secure evidence-transfer methods.

Each provider-dependent objective should have a named provider contact and a contractor owner. If the provider cannot support a requested demonstration or evidence type, the team should identify an alternative supported by the actual implementation or resolve the deficiency.

The conference should produce a written action list. This prevents the contractor from discovering on assessment day that a provider requires ten business days to produce a report or that the only engineer with console access is unavailable.

Substantive Depth Pass — Assessment-Day Evidence Control

The evidence coordinator should maintain a live request register. Every request receives a unique identifier, requirement/objective reference where known, request description, owner, due status, artifact supplied, delivery time, and follow-up notes.

Before an artifact is supplied, a second person should verify that it is responsive, belongs to the correct environment, contains the expected period, and does not expose unnecessary unrelated information. This is quality control, not an attempt to filter unfavorable evidence.

If an assessor asks a follow-up question, the coordinator should link it to the original request. This creates an audit trail of the assessment interaction and prevents multiple teams from independently supplying different versions of the same evidence.

Substantive Depth Pass — Party ABC End-to-End Assessment Week

On the evening before assessment, Party ABC does not make broad configuration changes. It verifies participant availability, evidence-repository access, demonstration accounts, conferencing, and the request log. Party IJK confirms the engineers responsible for identity, endpoint, SIEM, vulnerability, and backup demonstrations.

On the first assessment day, ABC's coordinator presents the environment and scope. Business personnel explain CUI workflows; IJK explains the technical components it

operates. When the assessor requests evidence, the request is logged and routed rather than answered by whoever happens to be speaking.

During a logging demonstration, the assessor asks how ABC knows a source has stopped reporting. IJK demonstrates source-health monitoring and a historical ticket. ABC's security owner explains the escalation expectation and business response. This combined answer shows the division between operation and accountability.

On the second day, a sampled endpoint appears in the inventory and EDR console but not in the most recent vulnerability report. Rather than guessing, the team records the question and investigates. It determines that the endpoint was added after the scan cutoff and shows its subsequent enrollment and scan evidence. The chronology explains the apparent discrepancy without changing the historical record.

At the end of each day, ABC reviews open requests and the next day's schedule. The team does not rehearse answers based on what the assessor asked; it ensures the correct people and records will be available. The assessment remains an evaluation of the operating program.

Substantive Depth Pass — Management Readiness Memorandum

Before committing to the assessment, management should receive a written readiness memorandum. It should summarize the contractual requirement, current implementation context, assessment scope, systems and providers, unresolved findings, evidence completeness, interview readiness, demonstration readiness, provider readiness, and logistics.

The memorandum should identify any assumptions explicitly. For example, if a provider evidence item is expected but not yet received, management should see that dependency rather than a green status that hides it.

The readiness decision is not a guarantee of an assessment outcome. It is a documented management conclusion that the organization has performed a disciplined internal review and believes the environment, evidence, people, and provider relationships are prepared for evaluation.

Substantive Depth Pass — Continuous Readiness After the Assessment

Assessment preparation should leave behind an operating system for continuous readiness. The objective readiness matrix becomes an evidence-maintenance map.

The interview roster becomes a responsibility map. The demonstration runbooks become validation procedures. The recurring evidence calendar becomes part of security operations.

DFARS 252.204-7021 requires contractors subject to the clause to maintain the applicable current CMMC status for covered systems during contract performance and includes annual affirmation requirements for applicable CMMC UIDs. Readiness therefore cannot end when an assessment event ends.

The long-term goal is that a future assessment requires organization and validation, not reconstruction. If the company can preserve scope discipline, current SSP narratives, recurring evidence, provider accountability, and operational validation, assessment preparation becomes substantially less disruptive.

G.42 Authoritative Sources for Final Publication

Department CMMC Program - About CMMC (verified September 22, 2026). Current implementation status, Phase I/Phase II information, assessment overview, and POA&M overview.

CMMC Assessment Guide - Level 2. Official Level 2 preparation and assessment guidance, including assessment objectives and examine, interview, and test methodology.

DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025). Current-status definitions; CMMC UID; annual affirmation; SPRS; flowdown; Conditional-to-Final POA&M closeout obligations.

32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Program definitions, assessment requirements, scoping, POA&M provisions, affirmation, and related regulatory requirements.

Publication caution. CMMC implementation is currently under review. This appendix is an operational preparation guide, not a substitute for the controlling regulation, solicitation, contract clause, or current Department guidance. Re-verify these sources immediately before publication and before using the appendix for a specific procurement or assessment.

Appendix H
MSP Technician Security Checklist

Detailed Teaching and Field-Operations Edition

Authored by Dr. Charles Edwards

H.1 Purpose: The Technician as an Operational Control

CMMC readiness is not maintained only by executives, compliance personnel, or assessors. It is maintained every day by the people who create accounts, administer endpoints, approve or execute changes, investigate alerts, patch systems, restore data, manage remote access, and document what happened. For an MSP, the technician is therefore part of the customer's operating security system.

This appendix is designed to be used both as teaching material and as a field reference. The technician should understand not only what action is expected, but why the action matters, who has authority to approve it, what evidence should remain after the work is complete, and when the technician must stop and escalate rather than make an independent business or compliance decision.

H.2 The MSP Does Not Become the Contractor

An MSP can implement and operate important security mechanisms, but the contractor remains responsible for its contractual environment and business decisions. A technician should never assume that broad administrative access creates authority to make every decision.

For example, Party IJK may administer Party ABC's identity platform, but ABC should determine who is authorized for a business role. IJK may operate vulnerability tooling, but ABC may own outage approval and risk decisions. IJK may monitor security events, but ABC may own contractual reporting decisions. Clear separation prevents a technician from accidentally turning a technical action into an unauthorized business decision.

H.3 Current CMMC Context for MSP Operations

Current DFARS 252.204-7021 requires a contractor subject to the clause to maintain the required current CMMC status for covered contractor information systems used to process, store, or transmit FCI or CUI, and it includes annual affirmation and

flowdown obligations. This means technician activity can affect the operating condition that management later affirms.

The Level 2 Scoping Guide also recognizes Security Protection Assets and explains that an External Service Provider providing a security function, such as SIEM, may contribute to meeting requirements even if it does not itself process CUI. Technicians therefore need to understand whether the tools they operate are inside the relevant security architecture and whether their records may become assessment evidence.

H.4 The Technician's Five Questions Before Making a Change

Before performing security-sensitive work, the technician should answer five questions. First, am I working in the correct customer's environment? Second, am I authorized to perform this action? Third, does the change affect CUI, FCI, security protection, scope, or documented configuration? Fourth, what approval, testing, rollback, or evidence is required? Fifth, what must be documented when the work is complete?

These questions are intentionally simple. They prevent many common MSP failures: making a correct change in the wrong tenant, using broad privilege without customer authorization, disabling a security mechanism to solve an application problem, or completing technically successful work without leaving evidence.

H.5 Customer Separation Is a Security Requirement of MSP Operations

Party IJK may use shared management platforms to support Party ABC and Party EGH, but operational efficiency must never become customer-data commingling. Tickets, credentials, exports, screenshots, scripts, reports, and evidence should remain associated with the correct customer.

Technicians should verify the tenant, organization, device group, vault entry, and ticket before executing privileged work. When copying commands or scripts between customers, remove customer-specific identifiers and confirm that the configuration is appropriate for the destination. A standardized process is valuable; blindly duplicating one customer's configuration into another is not.

H.6 Named Technician Identity and Accountability

Privileged work should be attributable to an individual wherever the architecture permits. Named administrative identities improve accountability, investigation, access review, and evidence. A shared credential may make an action technically possible while making it difficult to determine who performed it.

Where a legacy platform forces use of a shared or emergency account, the MSP should treat that as an exception requiring stronger control: restricted vault access, checkout logging, MFA where possible, session logging, approval, rotation, and review. The technician should not create a new shared administrator account simply because it is convenient.

H.7 MFA and Privileged Authentication

Technicians should use approved multifactor authentication on applicable administrative and remote-access paths. They should never approve unexpected MFA prompts, share factors, enroll another person's device, or bypass MFA through an undocumented workaround.

If MFA prevents legitimate administration, the response is not to disable it silently. The technician should open or update the appropriate ticket, verify the identity and business need, use an approved recovery or break-glass process, and document the event. Repeated MFA failures may indicate a configuration problem or an attack and should be escalated accordingly.

H.8 Privileged Access Workstations and Administrative Devices

Administrative activity should originate from approved, managed devices appropriate to the customer's architecture. A technician's personal computer, unmanaged home device, or borrowed workstation should not become an emergency administrative platform simply because it is available.

The MSP should know which technician endpoints are authorized, how they are patched, protected, encrypted, monitored, and authenticated, and what happens if one is lost or compromised. If the MSP uses a dedicated privileged-access workstation model, technicians should understand which tasks require it and should not move privileged workflows to ordinary devices for convenience.

H.9 Remote Monitoring and Management Tools

RMM platforms are powerful because they can execute commands, install software, transfer files, access consoles, and change many systems. Those same capabilities make them security-sensitive. Technician access should be least-privileged, strongly authenticated, monitored, and limited to authorized customer groups.

Technicians should avoid using RMM file-transfer functions as an informal way to move CUI or sensitive evidence. They should know whether the platform is approved for the type of data involved. Scripts executed through RMM should be controlled, reviewed when appropriate, and documented when they materially change security configuration.

H.10 Credential Vaulting and Secret Handling

Customer administrative passwords, API keys, service-account secrets, recovery codes, certificates, and encryption keys should be stored only in approved systems. Technicians should not place secrets in ticket comments, personal notes, chat messages, spreadsheets, source-code repositories, or browser text files.

A technician who discovers an exposed secret should treat the exposure as a security event requiring containment and rotation according to the organization's process. Deleting the visible copy without evaluating where else the secret may have been replicated is not sufficient.

H.11 Customer Onboarding: Security Starts Before the First Ticket

When Party IJK onboards a new customer, technicians should not immediately deploy tools without understanding the approved scope and architecture. Onboarding should establish authorized contacts, administrative access, tenant boundaries, asset inventory, network information, identity sources, endpoint standards, logging sources, backup responsibilities, vulnerability processes, escalation paths, and evidence expectations.

The technician's work should produce a baseline that can later be reconciled. If 85 endpoints are expected at onboarding, the team should be able to explain why RMM, EDR, vulnerability, encryption, and patch populations differ. Unexplained population differences should be investigated.

H.12 User Onboarding

A user account should originate from an authorized request. The technician should verify the requester, assigned role, required groups, licenses, remote-access need, MFA enrollment, and any privileged access separately.

The ticket should show authorization and completion. The technician should not copy every group from a convenient existing user unless the customer's approved procedure explicitly supports that method and the resulting access is reviewed. Copying access can silently reproduce excessive privilege.

H.13 User Transfers and Role Changes

A role change is both an addition and a removal event. Technicians often focus on granting the new access while leaving the old access intact. The correct workflow should evaluate what the user no longer needs.

The record should identify who authorized the change, which memberships were added, which were removed, whether privileged access changed, and when the change occurred. High-impact transfers may require review of application-specific permissions outside the central directory.

H.14 User Offboarding

Termination and separation workflows should be time-sensitive and coordinated with the customer. The technician should know who can authorize disablement, what systems must be addressed, how sessions and tokens are handled, how remote access is revoked, how privileged credentials are removed, and how customer data on assigned devices is preserved.

Offboarding should also address shared resources, service ownership, forwarding, device return, and any MSP-managed application accounts. Closing the central identity account while leaving an active VPN, SaaS account, or local administrator identity is incomplete.

H.15 MSP Technician Departure or Role Change

When an MSP technician leaves Party IJK or changes duties, the MSP must treat the event as a multi-customer privileged-access change. Access should be removed from the MSP's own systems and from customer-specific systems, portals, vaults, VPNs, cloud tenants, RMM groups, backup platforms, SIEM tools, and vendor consoles.

The MSP should maintain enough inventory of technician access that offboarding does not depend on memory. Shared secrets accessible to the departing technician should be evaluated for rotation according to policy and risk.

H.16 Endpoint Provisioning

A new endpoint should enter the environment through a controlled build or enrollment process. The technician should verify operating-system support, patch state, encryption, EDR, RMM/MDM, vulnerability coverage, firewall configuration, approved applications, local administrator restrictions, logging, and required identity controls.

The endpoint should not be considered complete merely because the user can sign in. Security-agent health and management enrollment should be validated. Evidence may include deployment records, management-console status, configuration profiles, and the onboarding ticket.

H.17 EDR and Security-Agent Health

Installing an EDR agent is different from maintaining effective EDR coverage. Technicians should monitor whether agents are healthy, communicating, licensed, policy-assigned, and current. A stale or disconnected sensor should generate operational follow-up.

When an agent interferes with an application, the technician should not disable or uninstall it without an authorized troubleshooting and exception process. The correct response may involve vendor support, policy tuning, exclusions approved through security review, or controlled testing. The final ticket should explain the decision and evidence.

H.18 Patch Management

Patch management requires more than clicking deploy. Technicians should understand the approved maintenance schedule, affected assets, prerequisites, testing, backup or rollback considerations, deployment result, failures, and verification.

Failed or deferred patches should remain visible. A technician should not mark a ticket complete because the deployment job was launched. Completion means the intended systems reached the expected state or the exceptions were documented and escalated.

H.19 Vulnerability Remediation

A vulnerability finding should move through ownership, analysis, remediation, validation, and closure. The technician should preserve the relationship between the original finding and the corrective work. Where a patch is unavailable or disruptive, the technician should escalate for an authorized decision rather than silently accepting the risk.

After remediation, validation should use an appropriate rescan or equivalent technical confirmation. A closed ticket without verification can create false confidence and weak assessment evidence.

H.20 Configuration Baselines and Drift

Technicians should know the approved baseline for systems they manage and how deviations are detected. Baselines may include operating-system settings, security policies, firewall configuration, logging, encryption, browser settings, services, applications, and administrative controls.

A deviation discovered during troubleshooting should not automatically become the new standard. The technician should determine whether it is authorized, temporary, customer-specific, or evidence of drift. Permanent baseline changes should follow change control and documentation updates.

H.21 Change Management

Security-sensitive changes should have a record of purpose, authorization, affected systems, implementation steps, testing, rollback, result, and evidence. The amount of documentation can scale with risk, but high-impact administrative changes should never become invisible work.

Emergency changes may need to occur quickly. Emergency does not mean undocumented. The technician should record what happened and ensure retrospective review according to the customer's process.

H.22 Logging and SIEM Operations

Technicians supporting logging should verify both configuration and health. A source configured months ago may no longer be sending useful data. Source heartbeat, ingestion status, time synchronization, parsing, retention, and alert routing should be monitored as applicable.

If a critical source stops reporting, the technician should open or trigger a tracked response, restore service, determine the period of missing visibility, and document the result. Simply restarting an agent without recording the monitoring gap loses important operational evidence.

H.23 SOC Alert Handling and Escalation

An MSP or MSSP technician should understand the difference between technical triage and customer decision authority. The provider may validate an alert, collect context, isolate a device under preauthorized conditions, and escalate. The customer may retain authority over business shutdown, legal decisions, customer notification, or contractual reporting.

Tickets should preserve chronology: detection time, analyst actions, customer contact, containment, escalation, decision, and closure. If an alert suggests compromise of CUI or a covered system, technicians should follow the defined incident process rather than improvising external reporting.

H.24 Backup Monitoring

Backup technicians should monitor job status, capacity, repository health, credentials, encryption, and failures. Repeated warning states should not be normalized simply because most jobs complete.

The technician should know which systems and data are expected to be protected and should reconcile that expectation against the backup platform. A successful platform can still omit an important system if onboarding or configuration failed.

H.25 Restore Testing

Restore testing proves recoverability. The technician should follow an approved test plan, select an appropriate recovery point, restore into a safe location, validate integrity, validate permissions where relevant, record errors, and obtain acceptance from the appropriate owner.

The evidence should be detailed enough that another person can understand what was tested. “Restore successful” without identifying what was restored or how it was validated is weak evidence.

H.26 Handling CUI and FCI During Support

Technicians may encounter CUI or FCI while troubleshooting, reviewing logs, accessing a user's device, restoring data, or collecting evidence. They should use only approved systems and transfer methods for the information involved.

A screenshot, memory dump, exported mailbox, log bundle, or backup sample can contain sensitive information even when the technician's purpose is purely technical. The support workflow should minimize unnecessary collection and place artifacts only in authorized locations.

H.27 File Transfer and Troubleshooting Artifacts

Technicians should resist the convenience of moving files through personal email, consumer storage, unapproved chat, or temporary public links. The approved transfer method should be known before sensitive troubleshooting begins.

Temporary diagnostic artifacts should have an owner and disposition. Once the support purpose is complete, unnecessary copies should be removed according to the applicable procedure while preserving records that must remain as evidence.

H.28 Removable Media

Use of removable media should follow the customer's approved policy and technical restrictions. A technician should not insert an unknown USB device into a covered system simply to move a driver or collect logs.

Where removable media is authorized, the technician should use approved media, follow scanning and encryption requirements, document use where required, and protect the media throughout the workflow.

H.29 Third-Party and Vendor Support Access

Vendor access should be authorized, time-bounded where appropriate, and monitored. Technicians should not provide a vendor with standing administrative credentials because it makes support easier.

The ticket should identify the vendor, purpose, approved access method, systems involved, start and end of access, actions performed, and removal or disablement. If the vendor requires a method that conflicts with the customer's security architecture, escalate before granting access.

H.30 Emergency and Break-Glass Access

Emergency access exists for exceptional conditions, not convenience. The process should define who can authorize use, how credentials are protected, what monitoring occurs, what actions are allowed, and what happens after use.

After a break-glass event, credentials or tokens may require rotation, logs should be reviewed, actions should be documented, and the event should receive retrospective approval or review. A break-glass account that becomes an everyday administrator account has failed its purpose.

H.31 Incident Recognition by the Technician

Technicians are often the first people to notice suspicious behavior: unexpected admin accounts, disabled security agents, unusual logins, encryption activity, unexplained outbound traffic, missing logs, repeated MFA prompts, or user reports of suspicious files.

The technician does not need to prove an incident before escalating. The responsibility is to recognize indicators, preserve relevant information, avoid destructive troubleshooting, and activate the defined incident process.

H.32 Evidence Preservation During an Incident

Ordinary troubleshooting sometimes destroys evidence. Reimaging a device, clearing logs, deleting suspicious files, or restarting services may eliminate information needed for investigation. Technicians should know when to stop routine remediation and obtain incident-response direction.

Preservation does not mean doing nothing. It means coordinating containment and recovery so that necessary evidence is retained according to the incident process.

H.33 Ticket Documentation as Security Evidence

A high-quality ticket tells the story of the work. It identifies the requester, authorization, affected system, problem or change, actions taken, timestamps, result, validation, exceptions, and closure. Attachments should be relevant and stored appropriately.

Technicians should write tickets so that another qualified person can understand what occurred months later. Vague entries such as “fixed,” “updated,” or “security issue resolved” provide little operational or assessment value.

H.34 Evidence Quality for MSP Technicians

Evidence should be attributable, contextual, and tied to the correct customer. Screenshots should show enough context to identify the setting without exposing unrelated data. Reports should identify the population and period. Exports should retain meaningful filenames and dates.

Technicians should never manufacture historical evidence or alter timestamps to make a process appear compliant. If a record is missing, report the gap and correct the process going forward.

H.35 Assessment-Time Technician Conduct

During an assessment, technicians should answer within their role, demonstrate the actual environment, and avoid speculation. If they do not know why a customer made a business decision, they should identify the customer owner rather than invent an answer.

Technicians should not silently change a configuration during an assessment to make a demonstration succeed. If a mechanism fails, the condition should be handled transparently through the assessment and remediation process.

H.36 What the Technician Must Never Do

Several actions should be treated as clear stop conditions: using another customer's credentials; placing CUI in personal email or unapproved storage; creating undocumented shared administrator accounts; disabling MFA, EDR, logging, encryption, or other security mechanisms without authorization; granting vendor access informally; using an unmanaged personal device for privileged administration; closing a vulnerability without validation; clearing potential incident evidence as ordinary cleanup; or fabricating assessment evidence.

The technician should also never assume that customer silence equals approval. When authorization is required and unavailable, escalate. A delayed change is preferable to an unauthorized security decision.

H.37 Daily Technician Checklist

- Verify you are operating in the correct customer tenant, ticket, vault, and device group before privileged work.
- Use only your approved named identity and approved administrative device.

- Respond to EDR/RMM/backup/SIEM health failures according to priority and escalation rules.
- Document security-sensitive changes and troubleshooting in the authoritative ticket.
- Protect CUI, FCI, credentials, screenshots, exports, and diagnostic artifacts using approved systems.
- Escalate suspected incidents and avoid destructive troubleshooting when evidence may be needed.
- Validate completed work rather than assuming a successful command or deployment job equals successful remediation.

H.38 Weekly Technician Checklist

- Review failed patch, backup, security-agent, vulnerability, and log-source health items assigned to you.
- Reconcile newly onboarded systems with required management and security tools.
- Review open privileged-access and vendor-access tasks for expiration or removal.
- Confirm unresolved security exceptions and deferred work remain visible and assigned.
- Review recurring tickets for systemic root causes rather than repeatedly fixing the same symptom.

H.39 Monthly Technician Checklist

- Participate in customer asset-population reconciliation where assigned.
- Review stale or unhealthy EDR/RMM/MDM/vulnerability/logging agents and resolve unexplained gaps.
- Review privileged access assigned to MSP technicians for the customer.
- Verify recurring restore tests, vulnerability cycles, and patch cycles are producing expected evidence.
- Identify baseline drift or recurring emergency changes that require engineering or management attention.

H.40 Quarterly Technician Checklist

- Support formal privileged-access review and remove access no longer required.
- Participate in restore testing and incident/tabletop exercises where assigned.
- Review customer-specific administrative runbooks and escalation contacts for accuracy.

- Validate provider evidence retrieval for services that may be needed in an assessment.
- Review break-glass use, standing vendor access, and long-lived exceptions.

H.41 Customer-Specific Technician Readiness Matrix

Area	Party ABC	Party EGH	Technician Verification	Evidence/Record
Authorized admin identities				
Approved admin devices				
RMM/remote access				
EDR coverage				
Vulnerability coverage				
Logging/SIEM				
Backup/restore				
Incident escalation				
Approved CUI transfer				
Vendor access process				

H.42 Security-Sensitive Ticket Template

Field	Required Technician Entry
Customer / tenant	
Requester / authorization	
Affected system(s)	
Security impact / CUI-FCI relevance	
Planned action	
Approval / change reference	
Implementation steps	
Validation performed	
Evidence attached / location	

Exception or residual risk	
Escalation / customer decision	
Closure date and technician	

H.43 Technician Escalation Decision Guide

Condition	Technician Action	Do Not
Possible security incident	Preserve relevant evidence and activate incident escalation.	Reimage/clear logs merely to restore service.
Security tool blocks business application	Troubleshoot under approved process; seek security exception/tuning approval.	Disable the tool silently.
Customer approval unavailable	Hold or use preauthorized emergency process if applicable.	Assume silence is approval.
Vendor requests admin access	Verify authorization, method, scope, duration, and monitoring.	Share standing credentials informally.
CUI encountered in diagnostic artifact	Use approved storage/transfer and minimize copies.	Email it to a personal or unapproved account.
Control fails during assessment demo	Report accurately and coordinate response.	Change configuration secretly to make the demo pass.
Remediation cannot be validated	Keep item open and escalate.	Close ticket based only on attempted action.

H.44 Party IJK Supporting Party ABC and Party EGH

Party IJK standardizes its technician workflow across customers but does not standardize away customer ownership. A technician beginning work for Party ABC selects ABC's tenant, ABC's vault entries, ABC's ticket, and ABC's approved change process. Later that day, the same technician may support Party EGH through the same RMM platform, but EGH's device groups, evidence, approvals, and escalation contacts remain separate.

Suppose both customers receive the same EDR platform update. IJK can use a common engineering package and common validation logic, but each customer receives its own change record and deployment evidence. If ABC has a legacy engineering application requiring an approved exclusion while EGH does not, the technician must preserve that difference rather than copying ABC's exception into EGH.

This model gives the MSP efficiency without destroying accountability. Shared tools and repeatable procedures are strengths only when customer authorization, customer configuration, customer evidence, and customer decisions remain distinct.

H.45 Field Checklist: Before Privileged Work

- Correct customer and correct ticket confirmed.
- Authorization and change window confirmed.
- Named privileged identity and MFA available.
- Approved administrative device and access path in use.
- Backup/rollback requirement considered.
- Potential CUI/FCI exposure understood.
- Evidence requirements understood.
- Customer/provider contacts available if escalation is needed.

H.46 Field Checklist: After Privileged Work

- Expected technical result validated.
- Security-agent/logging/backup health rechecked if affected.
- No temporary account, firewall rule, exclusion, token, file, or vendor session left unintentionally.
- Ticket updated with actions, times, results, and validation.
- Evidence stored in the correct customer repository.
- Exceptions and failed steps escalated rather than hidden.
- Follow-up task and owner established when work is not fully complete.

H.47 Technician Self-Review Before Closing a Security Ticket

Before selecting Closed, the technician should ask: Can another technician understand exactly what I changed? Is the customer's authorization visible? Did I validate the result? Did I leave any temporary access or exception behind? If this ticket were selected during an assessment six months from now, would the record support the explanation I would give? If the answer to any of these questions is no, the ticket is not ready to close.

H.48 Manager Review of Technician Security Operations

MSP management should periodically sample technician work rather than relying only on completion metrics. Review a selection of privileged changes, vulnerability remediations, offboarding tickets, security-agent failures, vendor-access events, and incident escalations. Evaluate authorization, technical correctness, evidence, validation, and customer separation.

The purpose is not punitive inspection. It is quality assurance. Patterns such as repeated undocumented emergency work, weak closure notes, recurring shared-account use, or security-tool exclusions may indicate that the operating process needs redesign.

H.49 Evidence Produced by Routine MSP Work

Technician Activity	Natural Evidence	Why It Matters
Account provisioning	Approved request, identity record, group membership, MFA status	Shows authorized lifecycle and access configuration.
Endpoint onboarding	RMM/MDM/EDR enrollment, encryption/patch status, ticket	Shows controlled device introduction.
Vulnerability remediation	Finding, ticket, change, rescan	Shows discovery-to-closure lifecycle.
Log-source repair	Health alert, ticket, restored ingestion, validation	Shows monitoring and recovery of visibility.
Restore test	Request, recovery point, restore result, integrity validation	Shows recoverability rather than backup job success.
Vendor access	Approval, access record, session/ticket, removal	Shows controlled third-party administration.
Offboarding	Termination request, disablement records, access removal	Shows timely lifecycle closure.
Incident escalation	Alert, chronology, actions, handoffs	Shows operational response and accountability.

H.50 Final Technician Standard

A strong MSP technician leaves the environment more secure, more understandable, and more defensible after every meaningful action. The technician works under authorization, uses attributable identities, protects customer separation, validates technical results, preserves evidence, documents decisions, and escalates when authority or risk exceeds the technician's role.

The most important habit is disciplined consistency. CMMC readiness is easier when good security operations naturally generate trustworthy evidence. The technician should not have to reconstruct six months of work for an assessment because the work was documented correctly when it happened.

H.51 Regulatory and Publication Note

This appendix is an operational teaching guide and does not replace the controlling contract, 32 CFR part 170, current DoD CMMC guidance, DFARS clauses, the applicable NIST SP 800-171 requirements, or customer-specific policy. The September 2026 edition was prepared with reference to the current DFARS 252.204-7021 clause and the DoD CMMC Level 2 Scoping Guide. Because program

implementation and contractual requirements can change, MSPs and contractors should re-verify authoritative sources before publication and before applying the checklist to a specific contract or assessment.

Detailed Expansion — Technician Privileged-Access Workflow

A technician should never treat privileged access as a permanent convenience. Privileged access begins with an authorized business need, is granted to a named identity, is limited to the systems and functions required for the work, is protected by the organization's approved authentication controls, and remains subject to review. The ticket or change record should make the authorization and purpose visible.

Before using privileged access, the technician should confirm that the request applies to the correct customer and system. In a multi-customer MSP, similar server names, tenant names, and management groups can create dangerous ambiguity. The technician should verify the customer context in the PSA/RMM, the target hostname or tenant, and the approved scope of work before making a change.

During the session, the technician should avoid using privileged credentials for ordinary browsing, email, or unrelated work. Administrative activity should occur through the approved administrative path. When the work is complete, the technician should document the actions performed, validate the intended result, record any unexpected condition, and close or update the ticket only after confirming that security protections remain enabled.

Emergency or break-glass access requires even greater discipline. Its use should be exceptional, logged, reviewed, and followed by credential rotation or other required recovery actions. The existence of an emergency account must not become an excuse for routine shared administration.

Detailed Expansion — RMM and Remote Support Security

For an MSP, the remote monitoring and management platform can become one of the most security-sensitive systems in the service architecture because it may provide administrative reach across many customer environments. A compromised RMM identity or poorly controlled automation can create cross-customer consequences.

Technicians should use only individually assigned RMM identities protected by the approved MFA method. Role permissions should match job responsibilities. Technicians who need endpoint support should not automatically receive unrestricted

server, network, security-console, and scripting privileges. Elevated RMM roles should be reviewed regularly and removed promptly when responsibilities change.

Scripts and automation require change discipline. A script that is safe for Party ABC may not be appropriate for Party EGH because operating systems, applications, maintenance windows, or security requirements differ. Technicians should test scripts, identify the intended target group, document the change, and confirm that the automation cannot unintentionally execute across another customer's devices.

Remote sessions should be traceable to a ticket or approved activity. Where the platform supports session recording, command history, or audit logging, the MSP should configure and retain those records according to its approved operating model. Unattended access should not mean unaccountable access.

Detailed Expansion — Customer Isolation in Shared MSP Platforms

Standardization is valuable, but customer separation is mandatory. Party IJK may operate a common PSA, RMM, documentation platform, credential vault, SIEM service, or vulnerability-management platform, yet each customer's identities, credentials, assets, evidence, tickets, reports, and authorization decisions must remain properly segregated.

Technicians should confirm customer context before exporting reports or screenshots. A report intended for Party ABC must not contain Party EGH hostnames, usernames, IP addresses, vulnerability findings, ticket details, or other customer information. Templates can be shared; customer data cannot be casually mixed.

Credential vaulting requires the same discipline. Customer credentials should be stored in the approved customer-specific location with role-based access. Technicians should not copy passwords into personal notes, browser password stores, chat messages, or unrelated ticket fields. Where privileged credentials are checked out or rotated automatically, the technician should follow the vault workflow rather than bypass it for convenience.

Evidence preparation is another separation point. A generic MSP procedure may support multiple customers, but customer-specific implementation evidence should be collected and delivered separately. The technician should always know whether an artifact is a provider-level artifact, a customer-specific artifact, or both.

Detailed Expansion — Secure Technician Workstation

The technician's workstation is part of the administrative trust chain. A technician who can administer customer systems should not perform that work from an unmanaged personal computer or from a device whose security posture is unknown. The approved workstation should be inventoried, patched, protected by endpoint security, encrypted where required, and configured according to the MSP's administrative baseline.

Local administrator rights on technician workstations should be restricted. Browser extensions, unsanctioned utilities, credential-dumping tools, consumer synchronization applications, and personal remote-access software can undermine the security of otherwise well-managed customer systems.

Technicians should lock the workstation when unattended and protect screens from unauthorized viewing when working with sensitive customer information. Downloads containing configuration exports, logs, screenshots, or CUI-related material should be stored only in approved locations and removed from temporary local locations when no longer needed.

If a technician workstation is suspected of compromise, the technician should stop using it for customer administration and immediately follow the MSP's incident process. Continuing to administer customers from a potentially compromised workstation can turn one endpoint incident into a multi-customer event.

Detailed Expansion — Endpoint Provisioning as a Security Pipeline

Endpoint security should be built into provisioning rather than added manually after deployment. Party IJK should define a standard sequence that establishes inventory enrollment, management agent installation, endpoint detection and response, approved configuration baseline, encryption, patching, vulnerability coverage, logging, and other required controls before the endpoint is considered production ready.

Technicians should verify enrollment rather than assume installation succeeded. The device should appear healthy in the relevant management consoles. An EDR installer completing successfully on the endpoint does not prove that the sensor is checking in. Likewise, an RMM agent can be installed while the device is assigned to the wrong customer group or policy.

The provisioning record should identify the device, customer, assigned user or purpose, date, technician, security tools applied, validation result, and any exception. Exceptions should have an owner and follow-up rather than becoming permanent undocumented gaps.

Retirement should reverse the lifecycle safely. Access should be removed, sensitive data handled according to policy, management records updated, credentials or certificates revoked where applicable, and the device removed from active operational populations without destroying records needed for evidence or audit history.

Detailed Expansion — EDR Health and Response Workflow

EDR operations require more than installing an agent. The technician should know how the MSP identifies unhealthy, disabled, outdated, or non-reporting sensors. A daily or automated health process should identify devices that have stopped communicating and create an actionable workflow.

When an EDR alert occurs, the technician must understand the boundary between routine support and security response. The technician should not delete evidence, reboot a system, remove files, or disable security tooling simply to restore service if those actions could interfere with incident investigation. The event should be escalated according to the incident-response procedure.

If containment is authorized, the technician should document who authorized it, what action was taken, when it occurred, and the resulting system state. If the MSP's SOC performs containment directly, the customer and support teams should understand the handoff and restoration process.

False positives should also be documented appropriately. Creating broad exclusions to stop recurring alerts can create a larger security weakness. Exclusions should be narrow, justified, approved, and periodically reviewed.

Detailed Expansion — Patch and Vulnerability Operations

Patching and vulnerability management overlap but are not identical. Patch management distributes updates; vulnerability management identifies weaknesses, determines applicability and priority, tracks remediation, and verifies closure. Technicians should understand both workflows.

When a vulnerability is identified, the technician should confirm the affected asset and current state before changing it. Remediation may involve a vendor patch, configuration change, software removal, upgrade, access restriction, or another approved action. The ticket should preserve the original finding and document the corrective action.

After remediation, verification matters. A successful patch deployment message does not necessarily prove the vulnerability is gone. Where practical, rescan or otherwise verify the corrected condition. Failed installations, systems awaiting reboot, incompatible applications, and devices offline during the maintenance window should remain visible until resolved.

Technicians should not close aged vulnerabilities merely because a dashboard needs to look clean. If remediation is blocked, escalate the dependency and maintain accurate status.

Detailed Expansion — SIEM, SOC, and Log-Source Health

Technicians often support the systems that feed a SIEM even when a separate SOC performs monitoring. They should understand that a configured log source is not necessarily a functioning log source. Service stoppage, certificate expiration, agent failure, firewall changes, storage limits, or configuration drift can silently interrupt telemetry.

When a log source is added, the technician should verify ingestion and, where applicable, parsing, timestamps, and source identity. The onboarding ticket should record that validation. For critical sources, the operating model should include a way to detect loss of telemetry.

If a SOC reports that a source has gone silent, the technician should treat the condition as a security service issue, not merely a reporting inconvenience. Troubleshooting should preserve relevant evidence and document the outage period, cause, correction, and validation.

Party IJK's technician should understand the escalation boundary: the technician may restore a collector or agent, the SOC may analyze security events, and Party ABC may own business decisions and contractual reporting. The ticket should make these handoffs visible.

Detailed Expansion — Backup and Recovery Technician Workflow

Backup administration must protect both availability and confidentiality. Technicians should know which systems and data are protected, how jobs are monitored, how failures are escalated, how backup administration is secured, and who can authorize restoration.

A failed backup should generate action. Repeatedly acknowledging the same failure without correcting the cause creates false assurance. The technician should determine whether the problem involves storage capacity, credentials, connectivity, application consistency, agent health, repository availability, or another dependency.

Restore testing should be performed in a controlled manner. The technician should document the requested recovery point, target location, restoration method, result, integrity checks, permissions checks, and any errors. Restoration should not expose CUI to an unapproved temporary location simply because it is convenient for testing.

Backup administrator credentials and encryption keys require special protection. A technician should never place recovery secrets in an ordinary ticket or chat conversation.

Detailed Expansion — Incident Recognition and First Technician Actions

The first technician to observe suspicious activity can materially affect the quality of the response. The technician does not need to determine conclusively that an incident has occurred before escalating a credible security concern.

Examples include impossible or unusual authentication activity, repeated MFA prompts, disabled security agents, unexpected administrator accounts, ransomware indicators, unusual encryption, suspicious PowerShell or scripting, unexplained log deletion, large unexpected data transfers, or a user reporting that credentials may have been disclosed.

The technician should preserve the current state where practical, record the time and observations, and follow the approved escalation channel. Actions such as deleting suspicious files, wiping logs, reinstalling the system, or broadly rebooting devices may destroy evidence or expand impact.

The incident record should distinguish observation from conclusion. “User reported 37 unexpected MFA prompts beginning at 09:12” is stronger than an unsupported statement that “the account was hacked.”

Detailed Expansion — Change Management for Security-Sensitive Work

Security-sensitive changes should have a clear reason, approved scope, implementation plan, validation method, and rollback consideration. Examples include firewall rules, identity policies, EDR exclusions, logging changes, privileged-group membership, backup configuration, vulnerability exceptions, and remote-access settings.

The technician should capture the pre-change state when useful. After implementation, the technician should verify both the intended function and the continued operation of relevant security controls. A firewall change that restores an application but breaks log forwarding is not a successful change.

Emergency changes may require expedited approval, but they should not become undocumented changes. The record should explain why the emergency path was used and should receive retrospective review according to the organization's process.

Assessment evidence is often produced naturally by good change management: authorization, chronology, configuration detail, validation, and ownership are already present in the ticket.

Detailed Expansion — Ticket Documentation as Security Evidence

A security-sensitive ticket should allow another qualified person to understand what happened without calling the original technician. It should identify the customer, asset or account, requestor, authorization, observed condition, work performed, timestamps where relevant, validation, residual issue, evidence reference, and closure decision.

Technicians should avoid vague entries such as “fixed,” “updated security,” or “checked logs.” Better documentation states what was changed and how the result was verified. For example: “Applied vendor update KBxxxx to ABC-SRV-04 during approved maintenance window; reboot completed; service health validated; authenticated vulnerability rescan no longer reports finding VULN-123.”

Tickets should not contain unnecessary secrets. Passwords, recovery keys, tokens, private keys, or CUI should not be pasted into ticket notes unless the approved system and process specifically permit the content.

Good tickets reduce assessment preparation because the evidence already exists as part of normal operations.

Detailed Expansion — Technician Actions During an Assessment

When supporting an assessment, technicians should answer only within their knowledge and responsibility. They should explain what they actually perform and demonstrate the actual environment. If another person owns authorization, policy, or contractual interpretation, the technician should identify that owner rather than speculate.

Technicians should never silently change a configuration because an assessor asks to see it. If the current state differs from the documented or expected state, the condition should be handled transparently through the assessment process.

Screenshots or exports created for the assessment should be checked for unrelated customer information. A technician working in a shared MSP console should confirm filters and tenant context before sharing a screen.

The assessment coordinator should manage requests. Technicians should not independently send multiple artifacts to different participants without ensuring that the evidence coordinator knows what was provided.

Detailed Expansion — Party IJK Technician Day: Party ABC

A Party IJK technician begins the day by reviewing security-sensitive alerts and failed automation for Party ABC. An endpoint has stopped reporting to EDR. The technician verifies that the device is still active in RMM and confirms the user is working remotely. Rather than reinstalling the agent immediately, the technician opens the existing health ticket, records the last EDR check-in, verifies the endpoint identity, and follows the approved repair workflow.

Later, the technician receives an approved request to add an engineer to a privileged application role. The technician verifies the Party ABC manager's authorization, confirms the requested role, performs the change using a named administrative identity, and records the resulting group membership. The technician does not add broader domain privileges because they were not requested.

During the afternoon, the SOC reports that a Windows server has stopped forwarding logs. The technician verifies service state, identifies a certificate issue, follows change procedures, restores forwarding, and confirms that new events appear in the SIEM. The ticket records the telemetry gap and restoration time. Each activity produces useful evidence because the technician followed the operating process rather than creating assessment-only documentation.

Detailed Expansion — Party IJK Technician Day: Party EGH

Party EGH is still preparing its environment and has not yet reached the operational maturity of Party ABC. The same Party IJK technician must therefore avoid assuming that ABC's procedures or approvals automatically apply.

When deploying a new EGH endpoint, the technician follows EGH's approved build profile and verifies EDR, encryption, patch policy, vulnerability enrollment, and logging. A required vulnerability agent does not enroll. The technician leaves the endpoint in a non-production state, opens a remediation item, and escalates rather than declaring the device complete.

Later, an EGH manager asks the technician through chat to disable MFA temporarily for a user who is having difficulty signing in. The technician does not make the change based solely on convenience. The request is redirected through the approved support and authorization process, and the underlying authentication problem is investigated.

This is the practical meaning of customer-specific accountability: the technician applies standardized professional discipline while respecting the authorization and security model of the individual customer.

Detailed Expansion — Technician Departure and Access Revocation

When an MSP technician changes roles or leaves the company, the offboarding process should account for the breadth of provider access. Removing the technician from the MSP's email system is not enough. The organization should identify RMM, PSA, documentation, vault, SIEM, EDR, backup, cloud, VPN, network, customer-local, and vendor-portal access associated with the individual.

Named identities should be disabled or removed promptly according to policy. Vault permissions and privileged roles should be revoked. API tokens, certificates, or keys personally assigned to the technician should be invalidated where applicable. Shared

or emergency credentials known to the departing technician should be evaluated for rotation.

The offboarding record should demonstrate completeness. Because MSP technicians can have access across many customers, incomplete offboarding is a cross-customer risk.

Detailed Expansion — Technician Quality Review

Party IJK should periodically review technician work for security quality, not merely ticket volume or closure speed. A sample review can examine whether authorization was documented, privileged access was appropriate, evidence was sufficient, validation occurred, customer context was correct, and secrets were handled properly.

Quality findings should feed training and process improvement. If several technicians omit post-change validation, the problem may be the ticket template or operational procedure rather than individual carelessness. If technicians repeatedly request broad administrative rights, role design may need improvement.

The goal is to make secure behavior the easiest standard workflow. A mature MSP does not depend on every technician remembering dozens of unwritten expectations under pressure.

Substantive Pass — A Complete Technician Shift From Login to Sign-Off

A secure technician shift begins before the first customer ticket is opened. The technician signs in from the approved managed workstation, confirms that required endpoint protections are healthy, uses the approved identity and MFA path, and reviews security-sensitive alerts, failed backup jobs, failed automations, unhealthy agents, open vulnerability work, and overnight escalations. The purpose is to identify conditions that can become larger problems if ordinary service requests consume the entire day.

The technician then reviews scheduled privileged changes and maintenance windows. Each activity should have an identifiable customer, approved scope, responsible owner, target systems, expected result, validation method, and rollback or escalation path. When several customers use similar names or shared MSP tooling, the technician deliberately confirms tenant and customer context before initiating work.

Throughout the day, the technician keeps security-sensitive activity tied to the PSA, change, incident, or remediation record. Privileged sessions are not performed as undocumented side work. Unexpected findings are recorded rather than silently corrected and forgotten. If the technician discovers a condition outside the approved scope, the technician stops and obtains direction before expanding the work.

At the end of the shift, the technician reviews unresolved security-sensitive tickets, pending reboots, failed patches, unhealthy EDR sensors, missing log sources, backup failures, and incidents awaiting handoff. The technician confirms that the next responsible person can understand the status without a telephone call. A secure end-of-day handoff is part of the control environment because unresolved work should not disappear between shifts.

Substantive Pass — Full Privileged Change Example

Party ABC requests a firewall rule change for an engineering application. The technician does not begin with the firewall console. The technician first verifies the authorized request, identifies the affected application and systems, reviews the requested source, destination, protocol, and port, and determines whether the change affects logging, segmentation, remote access, or another security mechanism.

Before implementation, the technician captures the relevant pre-change configuration or records the existing rule state. The technician uses a named privileged identity and the approved administrative path. The rule is implemented only for the approved scope; a broad “any-to-any” rule is not substituted because it is easier to troubleshoot.

Validation includes more than confirming that the application works. The technician confirms the intended traffic is permitted, unintended access has not been introduced, logging remains operational where required, and the rule appears correctly in the managed configuration. The ticket records the exact change and validation.

If the application still fails, the technician does not keep widening the rule until the problem disappears. The technician returns to troubleshooting and escalates if the approved change is insufficient. This prevents operational pressure from turning a controlled security change into an undocumented exposure.

Substantive Pass — Multi-Customer Security Incident

Party IJK's SOC detects suspicious use of an MSP technician account. Because the identity can access management systems supporting Party ABC and Party EGH, the

event must be treated as a potential provider-level incident with customer-specific impact analysis.

The first priority is containment according to the approved incident process. The affected identity is disabled or otherwise contained under authorized procedures, active sessions are reviewed, and alternate support coverage is established so emergency customer operations can continue. The MSP preserves identity, RMM, vault, VPN, endpoint, and administrative audit records relevant to the event.

The incident team then determines customer exposure separately. It asks whether the identity authenticated to ABC systems, EGH systems, both, or neither during the suspicious period. It reviews commands, remote sessions, credential retrieval, scripts, file transfers, configuration changes, and other available audit evidence. One customer's evidence is not mixed into another customer's incident package.

The technician team should not notify customers based on speculation, nor should it delay internal escalation because impact is uncertain. The approved incident leadership determines notification and contractual actions. Technicians provide accurate chronology and technical evidence.

Recovery includes credential rotation where required, restoration of trusted administrative access, review of technician endpoints, validation of RMM and vault integrity, and examination of whether role permissions were broader than necessary. The incident should produce corrective actions that address root cause rather than merely creating a replacement account.

Substantive Pass — RMM Compromise Response

An RMM compromise is particularly serious because the platform may provide scalable administrative reach. If suspicious RMM activity is detected, technicians should not treat the event as an ordinary endpoint ticket. The response should invoke the MSP's high-severity incident process and coordinate identity, platform, customer, and endpoint teams.

The team should preserve platform audit logs, authentication records, role changes, script execution history, remote-session records, policy changes, software deployments, and customer targeting information. It should determine whether malicious or unauthorized activity was limited to the management plane or reached customer systems.

Containment may include disabling identities, restricting administrative access, suspending automation, rotating secrets, isolating management infrastructure, or temporarily changing remote-support methods. These actions require coordinated authority because indiscriminately disabling the platform can also disrupt monitoring, patching, backup support, and incident visibility.

After containment, technicians validate customer systems independently. A clean RMM console is not sufficient evidence that endpoints were unaffected. The response may require endpoint telemetry review, configuration comparison, account review, persistence checks, and customer-specific validation.

The recovery decision should include management approval and a documented basis for restoring normal RMM operations. Lessons learned should address MFA, role design, administrative workstation security, vendor access, API tokens, automation controls, audit retention, and monitoring of the RMM itself.

Substantive Pass — Technician Evidence Package

For recurring security-sensitive work, Party IJK should define the evidence that a well-completed technician activity naturally produces. The objective is not to burden technicians with assessment paperwork; it is to make normal operational records sufficiently complete that they can later support customer oversight and assessment preparation.

For privileged account provisioning, the package may include authorization, ticket chronology, identity/group configuration, MFA status, and validation. For patching, it may include the original finding or update requirement, deployment record, reboot or service validation, and rescan or version verification. For a SIEM source repair, it may include the source-health alert, troubleshooting chronology, corrective change, restored ingestion, and closure validation.

For backup restoration, evidence may include authorization, selected recovery point, restore job, validation, and acceptance. For endpoint onboarding, it may include asset registration, RMM/MDM enrollment, EDR health, encryption, vulnerability enrollment, patch baseline, and technician sign-off.

Evidence should be customer-specific when it contains customer implementation information. Provider-level procedures can be reused, but customer records should remain separated and traceable.

Substantive Pass — Detailed Customer Onboarding Workflow

Before Party IJK administers a new customer, onboarding should establish both technical connectivity and governance. The MSP identifies the customer owner, authorized requestors, escalation contacts, systems in scope, permitted support channels, maintenance windows, emergency authority, evidence expectations, incident contacts, and applicable security requirements.

Administrative identities should be designed before broad access is granted. Named technician access, MFA, role groups, vault entries, remote-support paths, and logging should be established and tested. Default or temporary credentials should be removed or rotated according to the approved process.

The onboarding team inventories managed systems and reconciles them with RMM, endpoint security, vulnerability, backup, logging, and other applicable tools. Missing coverage becomes an onboarding issue rather than an accepted unknown.

The MSP documents customer-specific differences from its standard service model. Party ABC may authorize certain maintenance actions under standing change authority, while Party EGH may require explicit approval for each privileged change. Technicians need these differences visible in their workflow.

Onboarding is complete only when operational ownership is clear. The MSP should know who approves access, who receives alerts, who can authorize containment, who approves restoration, who owns contractual reporting, and who accepts residual operational risk.

Substantive Pass — Detailed Customer Offboarding Workflow

Customer offboarding is a security event as well as a commercial event. The MSP should establish an effective termination date, authorized contacts, data-return or transition requirements, credential handling, service shutdown sequence, evidence retention, and responsibilities for successor-provider coordination.

Technicians should remove or disable MSP access in a controlled sequence. This can include RMM agents, remote-support identities, VPN access, cloud roles, local administrator accounts, API tokens, certificates, vault entries, SIEM access, backup administration, and vendor portals. Removal should be verified rather than assumed.

Customer data held in MSP systems should be handled according to contractual and security requirements. Technicians should not delete historical evidence, tickets, logs,

or backups simply because active service ended unless the approved retention and disposition process calls for deletion.

Shared platforms require special care. Removing Party ABC must not disrupt Party EGH. Scripts, policies, monitoring rules, and integrations should be reviewed for customer-specific dependencies before deletion.

The final offboarding record should identify access removed, services transitioned, data disposition, unresolved issues, retained records, and the person who validated completion.

Substantive Pass — Daily Field Checklist Expanded

The daily checklist should function as an operational safety net rather than a ritual. At shift start, the technician confirms the health of the administrative workstation and approved access methods. The technician reviews security alerts, EDR health exceptions, failed backups, failed automation, critical log-source outages, urgent vulnerability items, and overnight incident handoffs.

Before each privileged activity, the technician confirms customer, authorization, target, scope, identity, and ticket. After each activity, the technician validates the intended result and confirms that related security mechanisms still function.

During the day, the technician watches for cross-customer context mistakes, unexpected privileged requests, attempts to bypass MFA or change controls, unapproved software, disabled security agents, suspicious user reports, and evidence that a system may be compromised.

At shift end, the technician reviews unresolved high-priority work, confirms ownership of every open security-sensitive issue, and records a handoff where necessary. No critical issue should depend on the next technician discovering it accidentally.

Substantive Pass — Weekly Field Checklist Expanded

Weekly review should look for patterns that daily work can miss. Technicians or team leads review unhealthy EDR and RMM agents, devices missing vulnerability coverage, repeated patch failures, recurring backup failures, stale privileged tickets, log-source health, aging security incidents, and exceptions approaching expiration.

The team should also review new customer assets and retired assets to ensure management populations remain aligned. Recently onboarded systems are sampled to verify that security tooling was applied correctly.

A small sample of technician tickets should be quality-reviewed for authorization, evidence, validation, customer context, and secret handling. Repeated documentation or workflow problems become training or process-improvement items.

Weekly review is also a good point to identify cross-customer provider problems. If the same agent version fails at three customers, Party IJK should create a provider-level engineering problem rather than treating each occurrence as an unrelated customer ticket.

Substantive Pass — Monthly Field Checklist Expanded

Monthly review should examine privileged access, technician role assignments, vault access, service accounts, emergency credentials, and provider administrative groups. Access no longer required should be removed.

Operational metrics should be reviewed for trends rather than vanity numbers. Useful questions include whether vulnerability age is increasing, whether patch failures repeat on the same systems, whether EDR health is deteriorating, whether backup failures are resolved promptly, and whether SIEM source outages recur.

The MSP should reconcile customer asset populations against key management systems. It should also review customer-specific exceptions, maintenance agreements, standing approvals, and escalation contacts for changes.

Monthly security operations should produce management information that explains where the service model is strong and where recurring technical debt or process weakness is accumulating.

Substantive Pass — Quarterly Field Checklist Expanded

Quarterly review should step above individual tickets and test whether the technician operating model remains effective. Privileged roles and customer access are recertified. Emergency access is reviewed. Representative restore tests, incident exercises, access reviews, and other recurring activities are completed according to the organization's procedures.

Party IJK should review whether customer responsibility matrices and operational contacts remain current. New services, cloud platforms, acquisitions, office moves, or staffing changes may alter responsibility and scope.

Technician training should address lessons from incidents, quality reviews, assessment findings, and technology changes. Training should be tied to actual operational problems rather than generic annual slides alone.

Quarterly review should also examine whether shared MSP platforms create new concentration risk. RMM, PSA, documentation, vault, SIEM, backup, and automation platforms should be considered from the perspective of what would happen if a privileged identity or platform were compromised.

Substantive Pass — Escalation Decision Framework

Technicians need a simple principle: escalate when the requested action exceeds authority, when security impact is uncertain, when evidence suggests compromise, when the action could affect multiple customers, when a control would be weakened, when contractual reporting may be implicated, or when the approved procedure does not cover the situation.

Escalation is not failure. A technician who pauses an unusual request protects both the customer and the MSP. The service culture should not reward technicians for solving every problem alone when doing so requires bypassing governance.

The escalation record should state the observed condition, action already taken, customer and systems affected, urgency, and the decision needed. This allows the next-level owner to make an informed decision quickly.

Substantive Pass — Security Exceptions and Temporary Workarounds

Operational pressure often creates requests for temporary exceptions: disable EDR for an installation, exclude a folder from scanning, postpone a patch, permit a legacy protocol, bypass MFA, or create a shared account. Technicians should never convert these requests into permanent configuration through informal action.

The exception should have a documented business reason, defined scope, approving authority, compensating operational treatment where appropriate, expiration or review date, and a plan to remove the exception. The technician implements only the approved exception.

Temporary workarounds should be visible in recurring review. An exception that expires without action should not silently become the new baseline. The technician workflow should generate a follow-up before expiration.

Substantive Pass — Evidence Preservation During Troubleshooting

Troubleshooting can destroy evidence if technicians immediately clear logs, uninstall agents, reset systems, or reinstall software. When the condition may involve security, the technician should first determine whether incident preservation procedures apply.

Useful preservation may include timestamps, screenshots, logs, process information, alert identifiers, system state, network observations, and ticket chronology. The technician should avoid collecting unnecessary sensitive information and should use approved repositories.

Once the incident or security owner confirms that ordinary remediation can proceed, the technician documents the corrective actions. This separation between observation and remediation makes the record much more useful for later investigation and assessment.

Substantive Pass — Technician Readiness Test

A technician is operationally ready when the technician can receive an unfamiliar but authorized task and execute it without losing customer context, bypassing security, exposing credentials, or creating an undocumented change. Readiness is demonstrated through behavior.

A practical readiness test gives the technician several scenarios: provision a privileged user, investigate an unhealthy EDR sensor, respond to a failed backup, handle a request to disable MFA, repair a silent log source, and recognize a suspicious administrative session. The evaluator observes how the technician verifies authorization, uses approved access, documents work, validates results, and escalates uncertainty.

The test should include a cross-customer trap, such as two similarly named servers in different tenants, to confirm that the technician verifies context rather than relying on memory.

Results should be used for coaching and process improvement. The purpose is to make safe execution repeatable under real service pressure.

Substantive Pass — Field Checklist: Before Privileged Work

- Confirm the correct customer, tenant, hostname, account, or management group.
- Confirm an approved ticket, change, incident, or other authorized work record exists.
- Confirm the requested action is within the technician's authority and assigned role.
- Use the approved managed administrative workstation and named identity.
- Confirm MFA and approved remote-access path are functioning.
- Retrieve credentials only through the approved vault or privileged-access process.
- Review security impact, dependencies, validation steps, and rollback/escalation plan.
- Capture the pre-change state when it will help validate or reverse the work.

Substantive Pass — Field Checklist: After Privileged Work

- Validate the requested function rather than assuming the command succeeded.
- Confirm related security protections remain enabled and healthy.
- Verify logs, monitoring, agents, and connectivity affected by the change.
- Record what changed, when, by whom, and under what authorization.
- Attach or reference appropriate evidence without exposing secrets or unrelated customer data.
- Record residual issues, required reboot, follow-up, exception, or dependency.
- Escalate unexpected security conditions instead of hiding them in closure notes.
- Close the work only when validation and required handoff are complete.

Substantive Pass — Closing Standard for the MSP Technician

The MSP technician is one of the most important operational participants in a CMMC-supporting environment because policy becomes reality through daily administrative work. Secure technician behavior is not achieved by asking technicians to memorize regulation numbers. It is achieved by designing workflows in which identity, authorization, customer separation, least privilege, evidence, validation, escalation, and accountability are built into ordinary service delivery.

Party IJK's objective should be that a technician can support Party ABC, Party EGH, and other customers efficiently without treating them as one environment. Standardization should improve quality while preserving customer-specific authorization and evidence. When this discipline becomes normal, the technician

checklist stops being an assessment preparation document and becomes what it should be: the operating standard for secure managed services.

Final Regulatory Verification and Publication Note

This Appendix H is an operational technician guide. It does not assign regulatory responsibility to an MSP technician or replace the contractor's System Security Plan, applicable policies, contractual requirements, or current CMMC program rules. Technician workflows should be mapped to the customer's approved environment, responsibility model, and contractual obligations.

The current November 2025 version of DFARS 252.204-7021 requires a contractor subject to the clause to have and maintain the applicable current CMMC status for covered contractor information systems used in contract performance that process, store, or transmit FCI or CUI. The clause also addresses CMMC UIDs, annual affirmations of continuous compliance in SPRS, subcontract flowdown, and successful closeout of a valid POA&M when the contractor has Conditional status. These are organizational and contractual obligations; the technician's role is to operate assigned services in a manner that supports the organization's implementation and evidence.

The official CMMC Level 2 Scoping Guide confirms that Security Protection Assets are within the CMMC Assessment Scope and are assessed against Level 2 security requirements relevant to the security capabilities they provide. The guide specifically gives an External Service Provider providing a SIEM service as an example of a security capability that can contribute to meeting CMMC requirements even when the service is logically separated and does not process CUI. This reinforces the Appendix H emphasis on RMM, SIEM, EDR, identity, backup, vulnerability, and other provider-operated security capabilities as systems that require disciplined administration, evidence, access control, and customer-specific responsibility mapping.

As of September 22, 2026, the Department's current CMMC program materials state that Phase II implementation was suspended on July 13, 2026 and that Phase I remains in place while the program is under review. This program change does not eliminate the need to protect covered information under applicable contractual requirements. MSPs and contractors should therefore recheck current CMMC program guidance, 32 CFR part 170, the applicable DFARS clauses, and the specific

solicitation, contract, task order, or flowdown before using this appendix for a particular procurement or assessment.

Authoritative Sources Used for Final Verification

- DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025), Acquisition.gov.
- CMMC Assessment Scope - Level 2, Version 2.13, Department CMMC program resources.
- Current CMMC About and Resources & Documentation pages, Department CMMC program, verified September 22, 2026.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program, as incorporated and referenced by current CMMC and DFARS materials.

Appendix I

Customer Onboarding and Offboarding Checklist

Detailed Teaching and Operational Transition Edition

I.1 Purpose of This Appendix

Customer onboarding and offboarding are security processes, not merely administrative events. An MSP can execute the commercial portion of a new relationship perfectly and still create serious security weaknesses if privileged access, customer scope, data flows, inherited accounts, security tooling, and responsibility boundaries are not established deliberately. The same is true at the end of the relationship: terminating billing does not terminate technical access, custody of information, or operational responsibility.

This appendix provides a teaching framework and field checklist for moving a defense contractor or other CMMC-relevant customer into and out of an MSP operating model. It is designed for MSP owners, service managers, security personnel, project managers, technicians, compliance teams, and customer representatives who must coordinate the transition.

I.2 The Core Principle: Secure Entry, Controlled Transition, Verifiable Exit

The onboarding objective is to establish a known and authorized operating state. The MSP should know what it is managing, who can authorize work, where FCI and CUI may exist, what systems and services are involved, what security functions the MSP performs, what remains the customer's responsibility, and what evidence the parties will maintain.

The offboarding objective is equally concrete. The parties should be able to demonstrate that services were transferred or terminated in an orderly way, customer information was returned or disposed of as authorized, MSP access was removed, successor-provider dependencies were addressed, and residual credentials or integrations did not remain active by accident.

The phrase “verifiable exit” is important. An MSP should not rely on a statement that access was removed. The closeout process should produce evidence showing what was disabled, removed, transferred, retained, or destroyed and who validated completion.

I.3 Commercial Onboarding Is Not Security Onboarding

The sales agreement, statement of work, recurring invoice, and kickoff meeting establish a business relationship, but they do not establish a secure managed environment. Security onboarding requires a second layer of work that translates contractual commitments into technical responsibilities and operational workflows.

A customer may believe that “the MSP handles cybersecurity,” while the MSP believes it only manages endpoints and Microsoft 365. Unless this ambiguity is resolved before privileged access and CUI-related services are operationalized, both organizations can make decisions based on incompatible assumptions.

For CMMC-supporting customers, the onboarding team should explicitly identify which security capabilities are supplied by the MSP or another External Service Provider, which requirements remain with the contractor, and what evidence each party is expected to maintain.

I.4 Current CMMC Program Context for Use of This Appendix

This appendix should always be used together with the current solicitation, contract, applicable DFARS clauses, 32 CFR part 170, and current Department CMMC program guidance. As of September 22, 2026, the Department's CMMC materials state that Phase II implementation was suspended on July 13, 2026 while Phase I self-assessment requirements remain in place and the program is under review.

The practical implication is that onboarding teams should not assume that every customer is following the same assessment path merely because the customer handles defense information. The MSP should record the customer's actual contractual requirements and current CMMC status rather than substitute a generic statement such as “CMMC Level 2 customer.”

I.5 The Parties in the Onboarding Model

Throughout this appendix, Party IJK represents the MSP. Party ABC represents an established defense contractor that has a comparatively mature security program.

Party EGH represents a smaller contractor entering Party IJK from another provider with incomplete documentation and inherited technical debt.

The examples are intentionally different. A strong onboarding method must work when the customer is organized and when the customer is not. The MSP should not lower its evidence or authorization standards simply because an incoming environment is poorly documented.

I.6 Establishing the Onboarding Authority

Before Party IJK changes a system, the MSP should know who is authorized to direct the work. The customer should identify executive sponsorship, operational contacts, authorized requestors, security contacts, incident contacts, and individuals who can approve privileged access or material configuration changes.

The MSP should also establish its own transition leader. This person coordinates technical discovery, service activation, security exceptions, unresolved dependencies, and the eventual handoff to steady-state operations. Without a transition owner, onboarding becomes a collection of disconnected tickets.

I.7 Contract and Responsibility Review

The onboarding team should review the statement of work, service descriptions, exclusions, security addenda, incident obligations, data-handling requirements, and subcontractor or provider dependencies. The purpose is not to turn technicians into contract attorneys; it is to ensure that the operational design reflects what the parties actually agreed to perform.

Responsibility should be expressed in operational verbs: who owns, who decides, who implements, who operates, who produces evidence, who maintains evidence, and who independently assesses where applicable. A vague statement that Party IJK “handles security” should be decomposed into specific services.

I.8 FCI and CUI Discovery

The MSP should ask where Federal Contract Information and Controlled Unclassified Information are created, received, processed, stored, transmitted, backed up, printed, exported, and archived. Discovery should include user workflows, not only servers. Important information may exist in email, Teams or collaboration sites, file shares,

engineering applications, cloud storage, local endpoints, removable media, scanners, multifunction devices, or third-party portals.

The MSP should document what the customer knows and what remains uncertain. Discovery is not improved by pretending that unknowns do not exist. Unknown repositories should become assigned investigation items.

I.9 Scope and Data-Flow Validation

Once information locations are understood, the team should map the systems, people, technologies, facilities, and external services that support the environment. Data-flow diagrams should show meaningful movement of FCI/CUI and the security services that protect those flows.

Party IJK should resist the temptation to define scope only by what it manages. The contractor's CMMC environment can include assets and services outside the MSP's management boundary. Conversely, an MSP-operated security capability can be important to the customer's security model even when it is logically separated from CUI.

I.10 Asset Inventory Reconciliation

An incoming inventory should be treated as a hypothesis until it is reconciled. Party IJK should compare customer records against directory services, RMM, MDM, EDR, vulnerability platforms, network discovery, cloud tenants, backup systems, virtualization platforms, and other authoritative sources.

Differences should be categorized: expected, retired, duplicate, unknown, unmanaged, or newly discovered. The goal is not merely to create a spreadsheet. It is to establish the population against which security coverage can later be measured.

I.11 Identity and Privileged Access Establishment

MSP administrative access should be designed rather than inherited casually. Party IJK should establish named technician identities, MFA, role-based groups, privileged-access procedures, vaulting, emergency access, and logging before routine support begins.

Legacy shared administrator accounts should be identified. Where they cannot immediately be removed, they should be treated as transition risks with an owner and

remediation plan. Technicians should not continue using an outgoing provider's shared credential simply because it works.

I.12 Customer Authorization Matrix

The authorization matrix tells technicians who may request what. Routine user support, new accounts, privileged access, firewall changes, security exclusions, restoration, incident containment, and emergency changes may require different approval authority.

This matrix should be visible to the service desk. A technician should not have to guess whether a person requesting an EDR exclusion is authorized to weaken a security control.

I.13 RMM, MDM, and Remote Support Deployment

Party IJK should deploy management agents through a controlled onboarding plan. Each device should be assigned to the correct customer, site, policy, and management group. Remote-access permissions should be validated and unnecessary inherited tools removed according to an approved transition sequence.

If the outgoing MSP's RMM remains installed temporarily, both parties should understand the overlap period. Two providers with unrestricted remote administrative access can create accountability and security problems unless the transition is explicitly controlled.

I.14 Endpoint Security and EDR Transition

EDR coverage should be reconciled against the asset inventory. Party IJK should identify endpoints without sensors, unhealthy sensors, policy mismatches, duplicate products, exclusions, and systems still reporting to the outgoing provider.

Replacing endpoint security should be staged carefully. Removing the old agent before the new protection is validated can create an avoidable protection gap. The onboarding record should show the transition and validation.

I.15 Vulnerability and Patch Baseline

A new customer should enter steady-state service with a known vulnerability and patch baseline. Party IJK should identify critical and aged vulnerabilities,

unsupported systems, missing patches, pending reboots, and systems excluded from normal maintenance.

Inherited findings should not be silently attributed to the new MSP, nor should they be erased to create a clean dashboard. The transition record should distinguish inherited conditions from findings generated after Party IJK assumes operational responsibility.

I.16 Logging, SIEM, and SOC Onboarding

The team should identify required log sources, collection methods, retention expectations, monitoring responsibilities, alert-routing paths, and escalation contacts. A source is not onboarded merely because a connector was configured; Party IJK should verify that events are arriving and are associated with the correct customer.

SOC and service-desk responsibilities should be explicit. The SOC may detect suspicious behavior while Party IJK technicians restore a failed log collector and Party ABC makes contractual reporting decisions.

I.17 Backup and Recovery Onboarding

Party IJK should identify what is backed up, where backups are stored, who administers them, retention settings, encryption, recovery objectives, and restoration authority. Existing backup jobs should be tested rather than accepted at face value.

The MSP should also identify data that is not protected. If an engineering workstation contains important CUI but is excluded from backup by design, that fact should be understood and owned rather than discovered during an incident.

I.18 Cloud, GCC, GCC High, and SaaS Administrative Boundaries

Where Microsoft commercial cloud, GCC, GCC High, or another SaaS environment is used, the onboarding team should identify the actual tenant and service architecture rather than relying on labels used in conversation. Administrative roles, guest access, external sharing, identity integration, logging, retention, and third-party applications should be reviewed.

The customer and MSP should document who controls the tenant, who holds privileged roles, and what happens if the MSP relationship ends. A customer should not discover during offboarding that a critical tenant or domain is controlled solely through an MSP-owned identity.

I.19 Network and Security Infrastructure

Firewalls, switches, wireless systems, VPNs, DNS, DHCP, certificates, network monitoring, and remote-access gateways should be inventoried with administrative ownership. Party IJK should identify unmanaged or unsupported devices and record configuration backup status.

The onboarding process should also capture dependencies such as ISP portals, registrar access, DNS hosting, certificate authorities, and vendor support accounts. These often become major offboarding problems when ownership is unclear.

I.20 Service Accounts, API Keys, Tokens, and Certificates

Human administrator accounts are only part of the access picture. Service accounts, application secrets, API keys, automation tokens, certificates, SSH keys, backup credentials, and integration accounts can preserve access long after an individual account is disabled.

Party IJK should inventory these credentials where they fall within the service scope, identify ownership, protect them in approved systems, and establish rotation expectations. This inventory becomes especially important during offboarding.

I.21 Incident Response Integration

The MSP and customer should agree on how security events move from observation to escalation. Contact methods, severity thresholds, after-hours procedures, containment authority, evidence preservation, and customer decision points should be documented.

A technician who detects suspicious activity at 2:00 a.m. should not need to search an old email thread to discover whom to call. The onboarding process should make incident escalation operational.

I.22 Evidence Repository and Record Ownership

The parties should identify where operational evidence will live. Tickets, vulnerability reports, access reviews, change records, backup tests, incident records, SIEM reports, and configuration evidence may reside in different systems.

The customer should understand which evidence is provider-level, which is customer-specific, how it can be obtained, and what happens to it when the

relationship ends. Evidence access should not depend entirely on continued subscription to the MSP's portal.

I.23 Inherited Deficiencies and Transition Risk Register

Incoming weaknesses should be documented in a transition risk register. Examples include unsupported operating systems, unknown administrator accounts, missing EDR coverage, stale firewall rules, weak MFA deployment, unmonitored systems, failed backups, undocumented cloud applications, or incomplete CUI discovery.

Each item should have an owner, priority, planned treatment, and status. This prevents the transition period from becoming an indefinite excuse for unresolved risk.

I.24 POA&M and Remediation Handoff

Where the customer maintains formal or internal remediation plans, Party IJK should understand which items require MSP action and what evidence is expected for closure. The MSP should not independently declare a CMMC POA&M item complete merely because a technical ticket was closed.

The technician or engineering team can provide implementation and validation evidence; the customer retains the organizational responsibility for its applicable status, assessment, and affirmation obligations.

I.25 Security Baseline and Configuration Acceptance

Before steady-state handoff, the parties should agree on the operational baseline for managed systems. This may include identity policies, endpoint security, encryption, patch settings, firewall configuration, logging, backup, approved software, remote access, and administrative standards.

Exceptions should be explicit. If Party EGH cannot immediately meet the standard because of a legacy application, the exception should be documented rather than silently incorporated into the baseline.

I.26 30/60/90-Day Stabilization Model

The first thirty days should emphasize discovery, access control, inventory reconciliation, urgent protection gaps, and service continuity. Days thirty-one through sixty should deepen configuration standardization, vulnerability remediation, logging, backup validation, and documentation. Days sixty-one through ninety should focus

on evidence quality, recurring operations, unresolved exceptions, responsibility confirmation, and transition to normal governance.

The exact timeline can vary, but the concept is useful: onboarding is a managed stabilization period rather than a single kickoff date.

I.27 Transition-to-Operations Gate

Onboarding should end with a deliberate acceptance gate. Party IJK and the customer review whether scope is understood, administrative access is controlled, critical tooling is healthy, responsibilities are documented, major inherited risks are assigned, escalation paths work, and recurring operational schedules are established.

Unresolved issues do not necessarily prevent service transition, but they should be visible. The acceptance record should distinguish accepted operational risk from forgotten onboarding work.

I.28 Party ABC Onboarding Scenario

Party ABC arrives with an SSP, current asset inventory, defined CUI enclave, existing EDR, SIEM, backup service, and a mature internal security lead. Party IJK does not replace these structures merely to standardize its service. Instead, it maps its services into ABC's existing governance.

During reconciliation, Party IJK discovers that three engineering laptops are in Active Directory and the vulnerability platform but absent from the incoming RMM inventory. The devices are investigated, ownership confirmed, and management coverage corrected. The discrepancy becomes evidence that reconciliation worked.

ABC also requires explicit approval for privileged firewall changes. Party IJK configures its PSA workflow so technicians can see this requirement before work begins. The result is an onboarding process that preserves ABC's governance while integrating Party IJK's operations.

I.29 Party EGH Onboarding Scenario: Incomplete Documentation

Party EGH arrives from another MSP with a spreadsheet containing server names but no reliable workstation inventory, several shared administrator credentials, uncertain backup coverage, and no current network diagram. Party IJK does not label the environment “fully onboarded” after installing RMM.

The first phase establishes safe administrative access and inventories systems. Party IJK discovers an old file server containing contract-related information that EGH management believed had been retired. The server still has active user access and is not protected by the expected endpoint tooling.

The discovery is escalated to EGH. The parties determine how the information should be handled and whether the server belongs within the protected environment. The inherited condition is documented rather than hidden. This is precisely why security onboarding must include discovery rather than simply deployment.

I.30 When the Outgoing MSP Still Controls Critical Services

Transitions frequently reveal that the outgoing provider controls DNS, registrar credentials, backup repositories, firewall licensing, cloud administrative accounts, or security portals. Party IJK should not attempt to seize or bypass those systems. The customer should establish authorized transfer with the outgoing provider.

The transition plan should list each dependency, current owner, intended owner, transfer method, target date, and validation. Critical services should not be cancelled until the replacement or transfer has been confirmed.

I.31 Beginning the Offboarding Process

Offboarding should begin with written authority identifying the effective termination or transition date and the person authorized to direct the closeout. The parties should establish whether services are ending completely or transferring to a successor MSP.

The offboarding manager creates a dependency list before disabling access. Removing a management agent too early can eliminate the very access needed to transfer configurations or validate successor coverage.

I.32 Offboarding Scope and Dependency Inventory

The MSP should identify every customer-specific service and access path: RMM, PSA/customer portal, documentation, vault, EDR, vulnerability platform, SIEM, SOC integrations, backup, cloud roles, VPN, local administrator accounts, network equipment, DNS, registrar, certificates, APIs, vendor portals, licensing, and automation.

The list should include provider-level systems containing customer records even if they are not directly installed in the customer's environment.

I.33 Data Return, Retention, and Disposition

The parties should determine what customer data must be returned, what records Party IJK must retain, what can be deleted, and when deletion is authorized. This includes configuration exports, documentation, ticket history, reports, logs, backup data, evidence packages, and any customer information stored in provider systems.

Offboarding should not create uncontrolled copies. Transfers should use approved methods and should be documented. Sensitive information should not be sent through personal email or an ad hoc consumer file-sharing service because the relationship is ending.

I.34 Successor MSP Handoff

When a successor provider is involved, Party IJK should cooperate through an authorized transition process. The goal is continuity without granting uncontrolled access. The customer should approve what information is shared and who may receive it.

A useful handoff includes current inventories, network and system documentation, service dependencies, known open issues, maintenance schedules, security-tool status, and necessary configuration exports. Passwords and secrets should be transferred through an approved secure method and rotated when appropriate.

I.35 Removing Privileged Access

Party IJK should remove named MSP identities, group memberships, local administrator accounts, VPN access, cloud roles, vault permissions, and other privileged paths. The team should verify removal.

The customer should also consider credentials the MSP knew but did not exclusively own. Shared passwords may need rotation even if the MSP account itself has been deleted.

I.36 RMM and Remote Support Removal

RMM removal should be coordinated with successor coverage and customer authorization. The MSP should identify all enrolled assets, remove agents as agreed, revoke platform permissions, and verify that no unattended remote-support path remains.

Automation, scheduled scripts, policies, and integrations should also be reviewed. Removing the visible agent while leaving an API integration or secondary remote tool active is not complete offboarding.

I.37 EDR, Vulnerability, and SIEM Transition

Security tooling should not be removed in a sequence that leaves the customer blind. Where the successor provider is deploying replacement EDR or logging, the parties should coordinate overlap and validation.

Party IJK should preserve or transfer authorized historical reports and evidence before access is terminated. The customer should understand what historical telemetry will remain available after the service ends.

I.38 Backup Transition and Data Custody

Backup offboarding requires special care because the MSP may retain copies of customer data after production access is removed. The parties should document whether backups are transferred, retained for a defined period, or destroyed according to authorization.

Encryption keys, restore credentials, and repository ownership must be addressed. The final record should make clear whether Party IJK can still restore or access customer data after termination.

I.39 Cloud Tenant and Domain Control

The customer should leave the relationship with control of its own tenant, domains, registrar, DNS, certificates, and other critical business infrastructure unless another authorized arrangement applies. MSP-owned administrative identities should be replaced by customer- or successor-controlled identities.

Party IJK should verify that removal of its roles will not lock the customer out. This is one area where sequencing matters more than speed.

I.40 Service Accounts, Tokens, Keys, and Integrations During Exit

Offboarding should include non-human access. API tokens, webhook secrets, certificates, service principals, SSH keys, backup agents, automation credentials, and vendor integrations associated with Party IJK should be revoked, rotated, or transferred as appropriate.

The final verification should look for residual access from provider networks or systems, not merely review the user directory.

I.41 Evidence and Assessment Records at Termination

The customer may need historical evidence long after Party IJK stops providing service. The transition should identify what evidence the customer receives, what Party IJK retains under its own record obligations, and what provider-level evidence cannot be transferred in full because it includes other customers.

Where provider evidence supports a customer's assessment narrative, the parties should establish a reasonable method for preserving the customer's ability to demonstrate the historical service without exposing unrelated customer information.

I.42 Final Access Validation

The closeout team should test whether Party IJK can still access customer systems through known paths. This includes named accounts, remote tools, VPN, cloud portals, network devices, vendor portals, and APIs.

A failed login can be useful evidence, but the broader objective is to reconcile the access inventory against actual removal actions. Unknown residual access should be investigated before final acceptance.

I.43 Party ABC Offboarding to a Successor MSP

Party ABC selects a successor provider. Rather than cancelling Party IJK's services immediately, ABC establishes a thirty-day transition window. Party IJK prepares inventories, current network documentation, open vulnerability items, backup status, logging dependencies, and approved configuration exports.

The successor deploys its management and endpoint tools in a controlled overlap. Once ABC validates successor coverage, Party IJK removes its RMM and administrative identities. Shared credentials known to Party IJK are rotated by ABC or the successor.

Backup custody receives separate sign-off. Historical ticket and evidence exports are delivered through an approved repository. At the end, ABC, Party IJK, and the successor review the access-removal matrix and unresolved items. This is a controlled transition rather than a simple service cancellation.

I.44 Offboarding When the Relationship Ends Abruptly

Not every relationship ends cooperatively. Even when termination is immediate, the MSP should follow an approved security and legal process rather than improvising. Customer data should not be withheld, deleted, or exposed as a reaction to a commercial dispute.

Technical staff should receive clear direction regarding what access to disable, what systems must remain operational, what records to preserve, and who is authorized to communicate with the customer. The security objective remains controlled separation.

I.45 Management Acceptance and Closure

The final offboarding package should summarize services terminated or transferred, data disposition, access removal, credentials rotated or transferred, remaining dependencies, retained records, and unresolved matters. Management representatives should acknowledge closure.

The purpose is not ceremonial paperwork. It creates a defensible record that Party IJK no longer exercises unintended administrative control over the former customer's environment.

I.46 Regulatory and Contractual Caution

DFARS 252.204-7021 places CMMC status and related contractual obligations on the contractor subject to the clause. An MSP can support implementation, operate security capabilities, and produce evidence, but onboarding documents should not imply that the MSP assumes the contractor's organizational certification or affirmation responsibility.

The applicable solicitation and contract should always control. Current CMMC implementation guidance should be rechecked because the Department's 2026 Phase II suspension means program rollout conditions can change while the underlying cybersecurity and contractual obligations continue to require careful attention.

I.47 Master Customer Onboarding Checklist

- Confirm executed agreement, service scope, exclusions, security requirements, and transition authority.

- Identify customer executive owner, authorized requestors, security contact, incident contacts, and escalation paths.
- Record applicable contract/CMMC requirements and current status rather than assuming a generic level.
- Map responsibility: owner, decision-maker, implementer, operator, evidence producer, evidence custodian, assessor.
- Discover FCI/CUI locations and workflows; record unknowns for investigation.
- Validate scope, data flows, external services, facilities, users, and security protection assets.
- Reconcile asset inventory against directory, RMM/MDM, EDR, vulnerability, cloud, network, and backup sources.
- Establish named MSP identities, MFA, vaulting, least privilege, emergency access, and audit logging.
- Create customer authorization matrix for routine and security-sensitive work.
- Deploy and validate RMM/remote support with correct customer grouping and permissions.
- Reconcile EDR coverage and transition from inherited tooling without protection gaps.
- Establish vulnerability and patch baseline; preserve inherited finding history.
- Onboard required logging/SIEM sources and validate ingestion and escalation.
- Validate backup jobs, retention, encryption, administration, and restore process.
- Inventory cloud tenants, privileged roles, domains, DNS, certificates, and SaaS dependencies.
- Inventory service accounts, API keys, tokens, certificates, SSH keys, and integrations.
- Integrate customer with incident response and after-hours escalation.
- Establish evidence repositories, record ownership, and customer access expectations.
- Create transition risk register for inherited deficiencies and unresolved dependencies.
- Map MSP work to remediation/POA&M items where applicable without assuming contractor accountability.
- Establish approved security baseline and document exceptions.
- Complete 30/60/90-day stabilization activities.
- Conduct transition-to-operations review and obtain management acceptance.

I.48 Master Customer Offboarding Checklist

- Obtain written termination/transition authority and effective date.
- Identify successor provider, if any, and approved transition contacts.
- Inventory every service, access path, integration, credential, and customer record held by the MSP.
- Define data return, retention, transfer, and disposition requirements.
- Export authorized customer documentation, evidence, and configuration records.
- Coordinate successor deployment before removing critical monitoring or protection where appropriate.
- Remove named MSP privileged identities and verify removal.
- Rotate or transfer shared credentials known to the MSP.
- Remove RMM and unattended remote-support paths; revoke platform/API access.
- Transition EDR, vulnerability, SIEM/SOC, and logging without unintended visibility gaps.
- Transition or dispose of backups and document remaining data custody.
- Transfer cloud tenant, domain, DNS, certificate, registrar, and vendor-portal control.
- Revoke or rotate service accounts, API tokens, keys, certificates, and integrations.
- Review automation and scheduled tasks for residual MSP dependencies.
- Preserve required historical evidence and clarify provider-level evidence limitations.
- Test known access paths after removal and investigate residual access.
- Document unresolved items and responsible owner.
- Complete final access-removal matrix and management acceptance.

I.49 30/60/90-Day Stabilization Checklist

Period	Primary Objective	Representative Exit Criteria
Days 1-30	Establish safe control and discover reality	Authorized access established; critical assets identified; urgent protection gaps assigned; incident contacts active.
Days 31-60	Standardize and remediate	Security tooling reconciled; logging and backup validated; major inherited weaknesses under active treatment; documentation improved.
Days 61-90	Prove recurring operations	Evidence quality reviewed; exceptions owned; recurring schedules active; responsibilities confirmed; steady-

		state acceptance completed.

I.50 Customer Transition Risk Register Template

ID	Condition	Customer/ Service Impact	Owner	Treatment	Target	Evidence/ Closure
TR-001	Example: unknown shared domain administrator	Privileged-access accountability	Customer + MSP	Identify dependencies; replace with named/managed access	Date	Ticket, account review, validation
TR-002	Example: backup job failing on engineering server	Recovery capability	MSP	Repair job and complete controlled restore test	Date	Job history, restore record
TR-003	Example: outgoing RMM still active	Dual administrative control	Customer	Coordinate removal after successor validation	Date	Agent inventory, removal evidence

I.51 Customer Authorization Matrix Template

Activity	Authorized Requestor	Required Approval	MSP Role	Evidence
Routine user support	Customer-designated contacts	Per service policy	Service Desk	Ticket
Privileged access change	Named security/IT authority	Explicit authorization	Security/Systems Admin	Approval + configuration record
Firewall/security control change	Named technical/security authority	Change approval	Network/Security Admin	Change record + validation
Incident containment	Per incident plan	Severity-dependent	SOC/MSP Incident Team	Incident record
Restore from backup	Named business/IT authority	Restore authorization	Backup Admin	Restore record + acceptance

I.52 Offboarding Access-Removal Matrix Template

Access/Service	Current Owner	Removal/Transfer Action	Validated By	Status/Evidence
RMM	Party IJK	Remove agents and revoke tenant access	Customer/Successor	
Cloud privileged roles	Party IJK named admins	Remove roles after successor access validated	Customer	
VPN	Party IJK technicians	Disable named accounts/certificates	Customer	
Credential vault	Party IJK	Remove customer vault permissions; rotate shared secrets	Customer/Successor	
Backup platform	Party IJK	Transfer/retain/ destroy per authorization	Customer	

I.53 Final Teaching Perspective

A mature MSP treats onboarding and offboarding as two ends of the same governance process. At entry, the MSP establishes authorized access, known scope, customer-specific responsibilities, secure operating methods, and evidence. At exit, it unwinds those relationships deliberately and proves that access and custody have been transferred or terminated.

The strongest outcome is not a completed checklist by itself. It is an environment in which Party IJK, Party ABC, or Party EGH can explain who controlled each important service, how that control was authorized, what evidence was produced, what changed during the relationship, and how the relationship ended without leaving hidden administrative access or unmanaged security dependencies.

I.54 Authoritative Sources for Publication Verification

This detailed teaching edition was prepared using current official CMMC and DFARS program materials verified on September 22, 2026. Before final publication, the regulatory note and any time-sensitive implementation statements should be reverified.

- Department CMMC Program - About CMMC and Resources & Documentation, verified September 22, 2026.
- DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025), Acquisition.gov.
- DFARS 204.7504, Solicitation Provision and Contract Clause, Acquisition.gov.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program, as referenced by current Department CMMC and DFARS materials.

Deepening Pass — Taking Over From Another MSP

A takeover should begin with a transition ledger rather than a collection of passwords. Party IJK should identify every service currently operated by the outgoing provider, the technical dependency, the current administrator, the transfer authority, the planned transfer date, and the evidence that will prove control has moved. This prevents a common failure in which the new MSP discovers weeks later that the former provider still controls a registrar, backup vault, firewall subscription, certificate, or tenant-level account.

The outgoing MSP's documentation should be validated against the environment. If a handoff spreadsheet says there are twelve servers but directory, virtualization, backup, and vulnerability systems collectively reveal fourteen, Party IJK should investigate the difference before accepting the inventory. The objective is not to criticize the prior provider; it is to establish a trustworthy starting point.

Administrative overlap should be time-bounded. During transition, both providers may require access, but the customer should know which provider is authorized to make which changes. When Party IJK assumes responsibility for a service, the outgoing provider's access should be removed or reduced according to the agreed transition plan.

Deepening Pass — CUI Discovery Workshop

A CUI discovery workshop should follow the customer's actual work. Rather than asking only “Where is CUI stored?”, Party IJK should ask how a contract arrives, who receives technical data, how employees collaborate, how engineering files move, how suppliers receive information, how users work remotely, what gets printed, where scans are saved, how files are backed up, and what happens when a project closes.

The workshop should identify systems and also human behaviors. A formally approved file repository does not prove that users never download material to desktops, email attachments to subcontractors, or copy files into an unsanctioned collaboration service. Discovery should therefore combine interviews, technical observations, and available system records.

Every uncertain location becomes a follow-up item. The team should distinguish confirmed CUI locations, likely locations requiring validation, and systems determined not to contain CUI. This improves both scope decisions and remediation planning.

Deepening Pass — Credential Ownership and Custody

A mature onboarding process distinguishes customer-owned credentials from MSP-assigned access. Party IJK should avoid becoming the sole custodian of credentials that the customer needs to retain control of its own business systems. Domains, cloud tenants, registrar accounts, certificate services, and other critical assets should have an ownership model that survives termination of the MSP relationship.

MSP technicians should use named identities whenever practical rather than a universal customer administrator account. Where a shared or application credential is unavoidable, the credential should be stored in the approved vault, access should be restricted, and rotation responsibility should be documented.

During offboarding, the question is not simply whether Party IJK deleted its accounts. The team must determine whether Party IJK still knows a shared password, possesses a certificate, retains an API token, or has an integration that can authenticate. These residual forms of access require rotation, revocation, or transfer.

Deepening Pass — GCC and GCC High Transition Planning

Cloud transition should begin by identifying the tenant that actually exists and the workloads actually used. The terms commercial, GCC, and GCC High should not be treated as interchangeable labels. Party IJK should document tenant ownership, identity architecture, administrative roles, licensing, domains, external sharing, mail flow, collaboration, endpoint integration, logging, and third-party applications.

If a customer is migrating between environments, onboarding should distinguish migration work from steady-state management. Mailboxes, collaboration sites, identities, applications, devices, and security tooling may transition on different

schedules. The project should identify when each workload becomes Party IJK's operational responsibility.

The MSP should also document what happens to source-environment data and administrative access after migration. A successful migration is incomplete if old privileged accounts or accessible repositories remain indefinitely without an approved retention purpose.

Deepening Pass — Inherited Technical Debt

Inherited technical debt should be visible before the customer and MSP begin measuring ordinary service performance. Party IJK should establish a baseline of unsupported operating systems, stale accounts, old vulnerabilities, weak configurations, failed backups, missing agents, undocumented applications, and other inherited conditions.

The baseline protects both parties. The customer receives a realistic view of the work required, while the MSP avoids creating the false impression that every inherited weakness arose after service began.

Technical debt should then move into normal governance. Each material item needs an owner, priority, target treatment, dependency, and evidence of closure. “Inherited” should describe origin, not justify indefinite acceptance.

Deepening Pass — 30-Day Stabilization

During the first thirty days, Party IJK should prioritize control over completeness. The MSP establishes authorized administrative access, validates incident contacts, reconciles critical assets, confirms security-tool coverage, identifies severe vulnerabilities, verifies backup status, and resolves immediate access or monitoring gaps.

The team should hold frequent transition reviews because new discoveries can alter earlier assumptions. A previously unknown server may change scope, backup requirements, vulnerability coverage, or data-flow diagrams.

At the end of the first thirty days, management should receive a stabilization report summarizing what was discovered, what was corrected, what remains unknown, and which inherited conditions require longer-term remediation.

Deepening Pass — 60-Day Standardization

Days thirty-one through sixty should convert the discovered environment into repeatable operations. Party IJK standardizes supported configurations, maintenance schedules, patch workflows, vulnerability remediation, logging, backup monitoring, privileged-access procedures, and ticket routing.

Exceptions should become explicit. Systems that cannot follow the standard process should have documented reasons and alternative handling. This is also the period to improve documentation, diagrams, customer authorization matrices, and evidence repositories.

The sixty-day review should ask whether the service is now predictable. If technicians still depend on tribal knowledge or a single employee to administer a critical system, stabilization is not complete.

Deepening Pass — 90-Day Operational Acceptance

By approximately ninety days, the focus should shift from deployment to proof of recurring operation. Party IJK should be able to show examples of completed patch cycles, vulnerability remediation, backup monitoring and restore activity, access administration, log-source health, change management, and incident escalation as applicable to the service.

The customer and MSP review unresolved transition risks and confirm responsibility boundaries. Any item that will remain open beyond onboarding should move into the appropriate steady-state risk, remediation, exception, or project process.

Operational acceptance should identify the date on which Party IJK's normal service metrics and governance replace transition reporting. This creates a defensible boundary between inherited conditions, transition remediation, and steady-state performance.

Deepening Pass — Successor MSP Handoff Package

A successor handoff package should be designed so the new provider can understand the environment without receiving unnecessary sensitive material. The package can include current asset inventories, diagrams, service dependencies, maintenance schedules, approved configuration exports, open security work, backup status, log-source information, and customer-specific operating notes.

Secrets should be transferred separately through an approved secure mechanism. The handoff package should not become a document containing every password and recovery key.

Party IJK should identify which records are snapshots and which remain subject to change during the transition. If the outgoing MSP provides an asset inventory two weeks before termination, the final reconciliation should account for devices added or retired during those two weeks.

Deepening Pass — Backup and Data Custody at Offboarding

Backups create a special offboarding problem because customer information may remain in provider-controlled repositories after all production access is removed. Party IJK and the customer should identify backup sets, retention periods, immutable copies, replication targets, encryption keys, and contractual retention or deletion requirements.

If backups are transferred, the receiving party should validate that restoration is possible. If they are retained temporarily, the agreement should identify who can authorize restoration and when final deletion will occur. If destruction is required, Party IJK should follow its approved destruction process and maintain appropriate evidence.

The closeout record should state plainly whether Party IJK retains any customer data after service termination. Ambiguity about backup custody is not a satisfactory offboarding state.

Deepening Pass — Proving Residual Access Has Been Removed

Final access verification should use the onboarding access inventory as its starting point. Each identity, role, VPN, RMM path, cloud account, vendor portal, API token, certificate, service account, and integration should have a corresponding disposition.

The team should sample or test critical paths after removal. For example, the former Party IJK cloud administrator should no longer appear in privileged roles; the RMM console should no longer show active customer devices; provider VPN credentials should fail; and customer firewall or backup portals should no longer accept MSP identities.

Residual access discovered after termination should be treated as a security issue and corrected promptly. The objective is evidence-based closure rather than confidence based on memory.

Deepening Pass — Party EGH: From Chaotic Takeover to Controlled Operations

Party EGH's first-week discovery identifies five separate administrator passwords stored in an old document, an unknown remote-support agent, two servers absent from the outgoing inventory, and a backup console controlled through the former MSP's email address. Party IJK creates separate transition items instead of trying to solve everything through one onboarding ticket.

The customer authorizes replacement named administrator identities and MFA. The unknown remote tool is investigated before removal to determine its owner and purpose. The two servers are classified and added to the asset and security-tool reconciliation. Backup ownership is transferred through the vendor rather than by sharing the former provider's mailbox credentials.

By day thirty, EGH has a trustworthy inventory and controlled access. By day sixty, endpoint, vulnerability, backup, and logging operations follow defined schedules. By day ninety, recurring evidence exists and remaining legacy issues have assigned owners. The scenario demonstrates that onboarding maturity is achieved through controlled discovery and stabilization, not through a single deployment weekend.

Deepening Pass — Party ABC: Controlled Exit With No Security Gap

Party ABC gives Party IJK notice that a successor MSP will assume operations. ABC remains the transition authority. Party IJK and the successor build a service-by-service sequence covering identity, RMM, EDR, vulnerability management, SIEM, backup, network administration, cloud roles, documentation, and vendor portals.

For endpoint security, the successor validates its agent population before Party IJK removes its product. For logging, ABC confirms that the successor can see required sources before Party IJK terminates monitoring. For backup, custody and historical retention are separately documented.

On the final day, Party IJK disables its named access, removes remaining remote-management paths, revokes tokens and integrations, and supplies the agreed evidence package. ABC rotates shared secrets known to Party IJK. A final access-removal

review confirms that the former provider no longer retains unintended administrative reach.

Deepening Pass — Onboarding and Offboarding Evidence Package

The transition evidence package should allow a reviewer to reconstruct what happened. Onboarding evidence may include kickoff authorization, responsibility matrix, initial and reconciled inventories, access records, security-tool deployment validation, risk register, data-flow updates, backup validation, incident contacts, and operational acceptance.

Offboarding evidence may include termination authority, successor handoff records, exported documentation, access-removal matrix, credential rotation confirmation, tool removal, backup disposition, data transfer, token revocation, final validation, and management closure.

The package should not contain unnecessary secrets or unrelated customer information. Evidence should demonstrate process without creating a new security exposure.

Deepening Pass — Management Decision Points

Management involvement is most valuable at defined decision gates. The first gate authorizes the transition and establishes scope. The second accepts the initial discovery and inherited-risk baseline. The third accepts steady-state operations. During offboarding, management authorizes termination, approves data disposition and successor handoff, and accepts final closure.

These gates prevent technical teams from silently making business-risk decisions. A technician can report that a legacy server cannot support the standard security agent; management and the appropriate customer owner decide how the exception will be treated.

Substantive Pass — The Onboarding Control Room

For a complex customer transition, Party IJK should run onboarding as a controlled program rather than a loose series of technician tickets. The transition leader maintains a master ledger containing services, systems, credentials, owners, dependencies, open risks, decisions, evidence, and target dates. Technical teams can

continue using normal PSA and project tools, but the master view prevents a critical dependency from disappearing between workstreams.

The control room concept is especially valuable when the outgoing MSP, customer staff, cloud vendors, security providers, and Party IJK all participate. Each transition item should have one accountable owner and a clear next action. Status such as "waiting" is incomplete unless the record identifies what is being awaited and from whom.

A daily transition review may be appropriate during the first several days. As the environment stabilizes, reviews can move to a weekly cadence. The goal is to reduce uncertainty systematically until the environment can enter normal operations.

Substantive Pass — Takeover Day Runbook

Takeover day should not begin with mass password changes. Party IJK first confirms the authorized transition window, customer decision-makers, outgoing-provider contacts, emergency communication channels, and the services that must remain uninterrupted. The team verifies that Party IJK has enough independent access to recover if one transfer step fails.

The runbook sequences high-risk dependencies. Domain and tenant administration, DNS and registrar control, firewalls, VPN, RMM, endpoint security, backup, SIEM, identity, certificates, and critical vendor portals should be handled in an order that preserves visibility and recoverability.

As each service transfers, Party IJK records the prior state, transfer action, new administrative owner, validation, and remaining legacy access. If a transfer fails, the team follows the predetermined rollback or escalation path rather than improvising under pressure.

The day ends with a reconciliation meeting. The team identifies services successfully transferred, services still shared with the outgoing provider, unresolved failures, credentials requiring later rotation, and any customer-impacting condition.

Substantive Pass — CUI Discovery Example: Engineering Workflow

Party EGH manufactures a component for a defense customer. Management initially states that CUI exists only on a secured file server. During the discovery workshop, Party IJK follows an engineering change from receipt to completion. The technical package arrives through an approved portal, is downloaded by an engineer, copied

into a project folder, opened in a CAD application, and discussed during collaboration sessions.

The engineer explains that large files are sometimes copied to a local workstation for performance. A multifunction device scans marked-up drawings into a network folder. A supplier receives selected technical files through a separate transfer mechanism. Nightly backup replicates the project server to a provider-managed repository.

The resulting data-flow map is much richer than the original statement “CUI is on the file server.” It identifies endpoints, collaboration, scanning, supplier transfer, backup, and user behavior that require analysis. Party IJK does not independently declare all of these assets in or out of CMMC scope; it provides the technical facts needed for the customer to maintain an accurate scope and SSP.

Substantive Pass — Cloud Tenant Transfer Runbook

Cloud-tenant transfer should establish durable customer control. Before changing roles, Party IJK identifies global or tenant-level administrators, emergency accounts, partner/delegated relationships, domains, subscriptions, billing dependencies, identity synchronization, application registrations, service principals, API permissions, security products, retention, and logging.

The customer confirms at least one authorized administrative path that does not depend solely on the outgoing MSP. Party IJK then establishes its named roles according to least privilege. Outgoing-provider roles are removed only after the new access path and critical services are validated.

Delegated administration requires separate review. Removing a visible user account does not necessarily remove partner-level delegated privileges or application consent. The team should inspect those relationships explicitly.

At offboarding, the process reverses: successor or customer access is validated, Party IJK's named and delegated roles are removed, application/service-principal access is reviewed, secrets are rotated where appropriate, and the customer confirms continued control.

Substantive Pass — Failed Transition Scenario: DNS and Registrar Ownership

Party EGH plans to move email and security services over a weekend. On Friday afternoon, the team discovers that the outgoing MSP's employee is the only person with registrar access and that the account recovery address belongs to the outgoing provider. Party IJK should not proceed as though DNS control is assured.

The transition leader escalates the dependency to EGH management and the outgoing provider. The customer establishes authorized ownership and recovery information before DNS-dependent migration steps occur. The schedule may need to change.

This example illustrates an important principle: delaying a transition because a critical control dependency is unresolved can be safer than completing a calendar milestone while ownership remains uncertain.

Substantive Pass — Failed Transition Scenario: Backup Looks Green but Restore Fails

During onboarding, Party IJK sees successful backup jobs for Party EGH and might be tempted to mark backup complete. A controlled restore test, however, fails because the application-consistent backup credential expired months earlier. The job dashboard had continued to show storage activity, but the required recoverable state was not available.

The condition is recorded as inherited technical debt. Party IJK repairs the credential and backup configuration, completes a new backup, performs a controlled restore, and documents validation. The onboarding record preserves both the inherited failure and the corrected state.

This scenario demonstrates why transition acceptance should be based on tested outcomes rather than console status alone.

Substantive Pass — Failed Transition Scenario: Residual Outgoing MSP Access

Two weeks after Party IJK assumes operations for Party EGH, a review finds that the outgoing MSP still has a delegated cloud administrative relationship. Its ordinary user accounts were removed, so the original offboarding checklist appeared complete.

Party IJK immediately escalates the finding to EGH and follows the approved process to remove the delegated relationship. Audit records are reviewed to determine whether the old provider used the access after the intended termination date.

The checklist is then improved to distinguish named users, groups, delegated administration, service principals, APIs, certificates, and other non-obvious access paths. A good transition program learns from discovered gaps.

Substantive Pass — Evidence-Based Operational Acceptance Criteria

Operational acceptance should require evidence in several categories. Governance evidence shows authorized requestors, responsibilities, escalation paths, and service ownership. Scope evidence shows reconciled assets, data flows, external services, and known CUI-related workflows. Access evidence shows named identities, MFA, vaulting, and privileged-role assignments.

Protection evidence demonstrates that applicable management, endpoint, vulnerability, logging, and backup services are deployed and healthy. Operational evidence demonstrates that recurring work is actually occurring. Risk evidence identifies unresolved inherited conditions, exceptions, and dependencies with assigned owners.

Acceptance does not mean the environment has no open issues. It means the parties understand the operating state and have deliberately assigned the remaining work.

Substantive Pass — Offboarding Control Room

Offboarding benefits from the same master-ledger discipline as onboarding. The transition manager tracks each service, data repository, access path, credential, integration, license, record set, and successor dependency through final disposition.

The offboarding ledger should distinguish “transferred,” “disabled,” “revoked,” “retained,” “destroyed,” and “not applicable.” A generic status of “complete” hides the information needed to prove what happened.

Daily review may again be necessary near the cutover date. The team should pay particular attention to actions that are irreversible, such as deleting a tenant object, destroying backups, terminating licensing, or removing the last administrative path.

Substantive Pass — Final Day Offboarding Runbook

On the final day, the team confirms successor/customer administrative access before removing Party IJK. Critical security services are checked for continuity. Open incidents and urgent vulnerabilities have explicit owners. Required evidence and documentation transfers are confirmed.

Party IJK then removes its access according to the access-removal matrix. Named accounts, VPN, RMM, cloud roles, delegated privileges, vault access, vendor portals, APIs, certificates, service accounts, and automation are addressed. Shared secrets known to Party IJK are rotated by the appropriate owner.

The team verifies customer control of domains, DNS, tenant administration, network equipment, backup, and other critical infrastructure. Data custody is reconciled, including retained backups or historical records.

Final closure occurs only after validation. If residual access is found, the offboarding remains open until the condition is corrected or formally assigned.

Substantive Pass — Customer Data Disposition Certificate

Where appropriate, Party IJK can use a customer data disposition record to document what happened to customer information held in provider systems. The record identifies categories of data, repositories, disposition action, effective date, authorization, retention exception, and validating person.

The record should not claim destruction when the MSP still retains immutable backups under an approved retention period. Instead, it should state the actual condition and planned expiration.

This type of record is particularly valuable when customer documentation, ticket attachments, configuration exports, or backup data reside in systems that the customer cannot inspect after termination.

Substantive Pass — Licensing and Subscription Transfer

Licensing can become a security dependency when products stop functioning after termination. Party IJK should identify whether security tools, cloud subscriptions, firewall services, certificates, backup capacity, or monitoring products are customer-owned, MSP-owned, or provided through a reseller relationship.

Before cancellation, the team determines whether the successor needs a new license, a tenant transfer, a grace period, or a replacement product. Security coverage should not disappear because a commercial cancellation date was processed before technical transition.

The offboarding package should record which licenses terminated, which transferred, and which remain customer-controlled.

Substantive Pass — Technician Handoff to Steady-State Service Desk

The service desk should not inherit a customer until technicians can find the information needed to support it safely. The handoff package should include authorized requestors, escalation contacts, customer-specific change rules, privileged-access method, maintenance windows, important architecture notes, security-tool locations, incident procedures, and known exceptions.

A handoff meeting should use real scenarios. The receiving technicians should demonstrate that they can identify the correct customer tenant, find approved credentials, recognize who can authorize a privileged change, and escalate a security event.

This converts onboarding documentation into usable operational knowledge rather than a project archive no technician reads.

Substantive Pass — Quality Assurance Sampling After Onboarding

Thirty to sixty days after steady-state handoff, Party IJK should sample actual service tickets to verify that the onboarding design is working. The review can examine privileged changes, new-user provisioning, endpoint onboarding, vulnerability remediation, backup failures, and security escalations.

If technicians are bypassing the customer authorization matrix or cannot find required documentation, the transition is not truly complete. The corrective action may involve documentation, PSA workflow, permissions, or training.

Post-onboarding QA closes the loop between project design and real operations.

Substantive Pass — Final Transition Evidence Index

A transition evidence index should identify each important artifact, its owner, location, date, customer relevance, and retention expectation. The index can point to rather than duplicate sensitive evidence.

Representative onboarding artifacts include the responsibility matrix, initial inventory, reconciled inventory, CUI/data-flow discovery notes, privileged-access record, security-tool coverage validation, transition risk register, restore test, incident contacts, and operational acceptance.

Representative offboarding artifacts include termination authority, successor handoff, access-removal matrix, credential rotation confirmation, RMM removal, cloud-role removal, backup disposition, data transfer, license transition, residual-access validation, and management closure.

Substantive Pass — Takeover-Day Field Checklist

- Confirm written transition authority, cutover window, customer decision-maker, and emergency contacts.
- Confirm outgoing MSP contact and escalation path.
- Verify independent customer/Party IJK administrative access before changing legacy access.
- Reconcile critical services: identity, tenant, domain/registrar, DNS, firewall/VPN, RMM, EDR, SIEM, backup, certificates, and vendor portals.
- Record which services remain under shared administrative control during transition.
- Transfer one service at a time where practical; validate before moving to the next dependency.
- Record new owner, access method, validation evidence, and remaining legacy access.
- Do not remove the outgoing provider's last recovery path until replacement access is proven.
- Hold end-of-day reconciliation and assign every unresolved dependency.

Substantive Pass — Operational Acceptance Checklist

- Customer authorization and escalation matrices are approved and accessible.
- FCI/CUI discovery has been performed and unresolved questions have owners.
- Asset inventory has been reconciled against major technical systems.
- Customer/MSP responsibility boundaries and ESP dependencies are documented.
- Named privileged identities, MFA, vaulting, emergency access, and audit paths are operational.
- RMM/MDM and endpoint-security populations reconcile to managed assets.

- Vulnerability and patch baseline is known; inherited findings remain traceable.
- Required log sources are validated and alert routing is operational.
- Backup scope is known and representative recovery has been validated where required.
- Cloud, network, domain, certificate, service-account, API, and vendor dependencies are documented.
- Incident response and after-hours escalation have been tested or reviewed.
- Transition risks and exceptions have owners and treatment paths.
- Recurring operational schedules are active and producing evidence.
- Service desk has completed customer-specific handoff.
- Management has accepted steady-state operations and remaining transition items.

Substantive Pass — Final Offboarding Verification Checklist

- Customer/successor has proven administrative control before Party IJK removes final access.
- All named Party IJK identities and privileged group memberships are removed.
- VPN, remote support, RMM, and unattended-access paths are removed and validated.
- Cloud delegated administration and partner relationships are reviewed and removed as applicable.
- Service principals, API tokens, certificates, SSH keys, and automation credentials are revoked, rotated, or transferred.
- Shared secrets known to Party IJK are rotated by the responsible owner.
- EDR, vulnerability, SIEM/logging, and backup services have transitioned without an unintended protection gap.
- Domains, registrar, DNS, cloud tenant, network equipment, and vendor portals are under authorized customer/successor control.
- Customer data transfer, retention, backup custody, and destruction status are documented accurately.
- Licenses and subscriptions have been transferred or terminated in the correct sequence.
- Historical evidence and required records have been delivered or retained according to the approved plan.
- Known former access paths have been tested or otherwise validated as removed.
- Residual access findings are resolved or explicitly assigned before closure.
- Final transition evidence index is complete.

- Customer and Party IJK management acknowledge closure.

Substantive Pass — Closing Perspective

Customer onboarding and offboarding are mirror-image security disciplines. Onboarding establishes authorized control; offboarding proves that control has been relinquished or transferred. In both directions, the strongest MSP process is based on inventories, responsibility, evidence, sequencing, validation, and explicit management decisions.

For Party IJK, success is not measured by how quickly agents can be installed or removed. It is measured by whether Party ABC or Party EGH can enter or leave the service relationship without losing visibility, protection, ownership, evidence, or control of its own environment. That standard turns transition management into an integral part of the MSP's security program rather than an administrative activity at the edges of it.

Final Regulatory Verification and Publication Note

This appendix is an operational onboarding and offboarding guide for MSPs and their customers. It does not replace the customer's System Security Plan, contractual requirements, current CMMC scoping determinations, legal advice, or the organization's responsibility for its own CMMC status and affirmations. The applicable solicitation, contract, task order, delivery order, and flowdown requirements remain controlling.

DFARS 252.204-7021 (NOV 2025) requires a covered contractor, when the clause applies, to have and maintain the applicable current CMMC status for contractor information systems used in contract performance that process, store, or transmit FCI or CUI. The clause also addresses annual affirmations of continuous compliance in SPRS, CMMC UIDs, subcontract flowdown, and successful POA&M closeout when a contractor has Conditional status. Appendix I therefore treats MSP onboarding records as supporting operational evidence rather than as a transfer of the contractor's organizational accountability.

The current CMMC Level 2 Scoping Guide states that use of an External Service Provider, the relationship to the Organization Seeking Assessment, and the services provided should be documented in the OSA's SSP and described through the ESP's service description and customer responsibility matrix. This supports Appendix I's

emphasis on explicit responsibility allocation during onboarding and preservation of those boundaries during offboarding.

As verified on September 22, 2026, current Department CMMC program materials state that Phase II implementation, originally scheduled for November 10, 2026, was suspended on July 13, 2026 and that Phase I self-assessment requirements remain in place while the program is under review. The same materials state that the pause does not eliminate the requirement to protect covered information under applicable DFARS requirements. Because implementation is changing, readers should recheck current official CMMC program guidance immediately before applying this appendix to a specific procurement, assessment, or transition.

Authoritative Sources Used for Final Verification

- DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025), Acquisition.gov.
- DFARS Subpart 204.75, Cybersecurity Maturity Model Certification, including the prescription for 252.204-7021 and 252.204-7025, Acquisition.gov.
- CMMC Assessment Scope - Level 2, Version 2.13, Department CMMC program resources.
- Current CMMC About and Resources & Documentation pages, Department CMMC program, verified September 22, 2026.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program, as referenced by current CMMC and DFARS materials.

Appendix J

Sample Incident Response Workflow

Detailed Teaching and Operational Edition

J.1 Purpose and Teaching Objective

Incident response is where security plans, technical operations, contractual obligations, evidence preservation, and management authority converge under time pressure. For an MSP, the difficulty is multiplied because the first person to see suspicious activity may be a technician or SOC analyst working in a provider platform, while the affected defense contractor retains organizational and contractual responsibilities.

This appendix provides a practical incident response workflow for MSPs supporting CMMC-relevant customers. It is designed to teach not only what steps occur, but why they occur, who is authorized to make decisions, what evidence should be created, and where the MSP must stop and escalate rather than assume authority it does not possess.

J.2 Incident Response Is a Business Process Supported by Technology

EDR, SIEM, firewalls, identity platforms, RMM, ticketing systems, and forensic tools can detect or help investigate suspicious activity, but none of them owns the incident. Effective response requires people, authority, communications, evidence, decision-making, and technical execution.

The workflow should therefore connect the SOC, service desk, security engineers, customer management, legal or contractual personnel where applicable, and other providers. A technically correct containment action can still create business or evidentiary problems if it is taken without appropriate authority or destroys information needed for investigation.

J.3 Event, Alert, Security Incident, and Reportable Cyber Incident

An event is an observable occurrence. An alert is a signal generated by a person or technology indicating that an event deserves attention. A security incident is an event or series of events that requires coordinated response because confidentiality, integrity, availability, or authorized operation may be affected.

A reportable cyber incident is a contractual concept that must be evaluated against the applicable contract and clause. Under DFARS 252.204-7012, when the clause applies, the contractor must rapidly report a cyber incident affecting a covered contractor information system or covered defense information, or affecting the contractor's ability to provide designated operationally critical support. The clause defines rapidly report as within 72 hours of discovery.

Party IJK should therefore avoid telling Party ABC that an EDR alert is automatically a reportable incident. Party IJK provides facts and technical analysis; Party ABC follows its approved decision and reporting process.

J.4 Current CMMC Incident Response Context

CMMC Level 2 includes incident-response requirements derived from NIST SP 800-171 Revision 2, including establishing an operational incident-handling capability, tracking and documenting incidents, reporting incidents to designated officials, and testing the organizational incident response capability.

The official Level 2 Assessment Guide evaluates whether these activities are implemented, not merely whether an incident response policy exists. This is why the workflow in this appendix emphasizes tickets, timelines, evidence, exercises, escalation records, and post-incident improvement.

J.5 The Incident Response Responsibility Boundary

Party IJK may monitor, detect, investigate, isolate endpoints, disable accounts, preserve logs, restore systems, and provide technical findings when those actions are within the authorized service scope. Party ABC or Party EGH remains responsible for organizational decisions that the contract, law, policy, or governance assigns to the contractor.

The boundary should be established before an incident. The incident plan should state who can authorize isolation of a production server, shutdown of a business application, disabling of an executive account, restoration from backup, engagement of outside counsel or forensics, notification to insurers, and contractual reporting.

During an incident, ambiguity consumes time. A responsibility matrix turns those decisions into a prepared process.

J.6 Preparation Before the Incident

The best incident response begins before the first alert. The customer and MSP should maintain current contacts, after-hours escalation, severity definitions, containment authority, evidence-handling procedures, logging and retention, backup and recovery procedures, and access to the systems needed for investigation.

The team should know how to contact the customer when email is unavailable or compromised. It should also know how to communicate securely if the normal collaboration platform is suspected of compromise.

Preparation includes testing. Tabletop exercises and technical exercises reveal missing phone numbers, inaccessible logs, weak authority definitions, and recovery assumptions before a real incident forces the issue.

J.7 Detection Sources

An incident may begin with an EDR alert, SIEM correlation, identity-risk notification, firewall event, vulnerability exploitation alert, backup anomaly, RMM activity, user report, service-desk ticket, cloud-provider notification, law-enforcement contact, customer observation, or another provider.

The source affects the initial evidence but should not determine the conclusion. A user saying “my computer is hacked” is an observation requiring triage. An EDR alert marked critical is also an observation requiring validation. The response team should establish facts before assigning a final classification.

J.8 First Technician Actions

The first technician should record what was observed, when it was observed, the affected customer, system or identity, the alert source, and any immediate business impact. The technician should avoid destructive troubleshooting, unnecessary rebooting, deleting suspicious files, clearing logs, or making broad configuration changes unless required by the approved containment procedure.

If immediate action is necessary to prevent material harm and the plan grants authority, the technician should act within that authority and document the action. If authority is unclear, the technician escalates quickly rather than improvising.

J.9 Initial Triage

Triage determines whether the observation is benign, a routine operational issue, a security event requiring investigation, or an incident requiring coordinated response. The analyst asks what happened, what asset or identity is involved, whether the activity is ongoing, what information may be affected, whether privileged access is involved, and whether the event could spread.

Triage should be time-aware. The purpose is not to complete a full forensic investigation before escalation. It is to gather enough reliable information to activate the appropriate response path.

J.10 Severity Classification

Severity should reflect potential impact, scope, privilege, sensitivity of information, operational disruption, and likelihood of continued harm. A single blocked malware execution on a non-sensitive workstation may follow a different path from suspected compromise of a domain administrator or MSP RMM account.

Severity is not static. A medium incident can become critical when investigation reveals CUI exposure or lateral movement. The incident record should preserve severity changes and the reason for them.

J.11 Incident Activation and Command

Once the threshold for coordinated response is met, the incident should have an incident lead. For MSP-managed technical response, Party IJK may provide the technical incident lead while the customer designates an organizational decision-maker.

The lead maintains priorities, assignments, communications, and the incident timeline. Technical specialists should not independently pursue competing theories without coordination because simultaneous unrecorded changes can destroy evidence or interfere with containment.

J.12 Establishing the Incident Timeline

The incident timeline begins with the earliest known relevant activity, not merely the time the ticket was opened. It should include detections, user reports, analyst observations, escalation, containment actions, account changes, system isolation, evidence acquisition, customer decisions, recovery steps, and communications.

Timestamps should identify the time zone. During a multi-party incident, a consistent time basis prevents confusion when SIEM, endpoint, cloud, and ticket systems display different time formats.

J.13 Evidence Preservation

Evidence preservation should begin early when compromise is plausible. Logs, alerts, endpoint telemetry, identity records, network data, relevant tickets, screenshots, configuration state, and other artifacts may become important.

Preservation does not mean collecting everything indiscriminately. The team should identify evidence relevant to the event and preserve it in a way that maintains integrity and access control. Technicians should avoid actions that unnecessarily overwrite volatile or historical evidence.

J.14 DFARS Media Preservation Considerations

When DFARS 252.204-7012 applies and a cyber incident is reported, the clause requires the contractor to preserve and protect images of known affected information systems and relevant monitoring or packet-capture data for at least 90 days from submission of the cyber incident report so DoD can request the media or decline interest.

This requirement is one reason an MSP technician should not automatically reimage a compromised system as the first response. The customer and incident team must consider evidence-preservation requirements before destructive remediation.

J.15 Containment Strategy

Containment reduces ongoing harm while preserving the ability to understand what occurred. Actions may include isolating an endpoint, disabling or restricting an account, blocking malicious indicators, revoking sessions, restricting remote access, segmenting systems, disabling an exposed service, or temporarily changing firewall rules.

Containment should be proportionate. Disconnecting an entire facility may stop an attack but may also create severe operational consequences. The incident lead should weigh urgency, spread, business impact, evidence, and available alternatives.

J.16 Identity Compromise Workflow

When an identity is suspected of compromise, Party IJK should examine authentication activity, MFA events, token or session behavior, privilege, recent account changes, mailbox or collaboration activity where authorized, and related alerts. The response may require session revocation, credential reset, MFA re-registration, temporary disablement, and review of privileged actions.

A password reset alone may be insufficient if active tokens, delegated permissions, application passwords, or attacker-created authentication methods remain. Recovery should therefore validate the complete identity state.

J.17 Endpoint Compromise Workflow

For a suspected endpoint compromise, the team identifies the device, user, network location, security telemetry, running or recently executed processes, persistence indicators, connections, and potential data exposure. EDR isolation can be valuable when authorized.

The response team should determine whether the endpoint is an isolated victim or evidence of broader compromise. Related identities, servers, file shares, remote connections, and management systems may need review before declaring containment complete.

J.18 Ransomware Workflow

Ransomware response begins with stopping spread and preserving evidence while protecting recovery capability. The team should identify affected systems, disable or restrict compromised identities, isolate systems where appropriate, protect backup administration, and determine whether the attack is still active.

Recovery should not begin until the team has reasonable confidence that the attacker’s access path and persistence have been addressed. Restoring clean data into an environment where compromised privileged access remains active can lead to immediate reinfection.

Business, legal, insurance, law-enforcement, reporting, and ransom-related decisions remain with the appropriately authorized parties. MSP technicians should not negotiate or make organizational commitments unless specifically authorized.

J.19 Suspicious CUI Transfer or Exposure

When telemetry suggests that CUI may have been transferred, accessed, or exposed improperly, the team should preserve the relevant records and establish facts: what data, which system, which identity, destination, time, transfer mechanism, and whether the action was authorized.

Party IJK should avoid making unsupported declarations that CUI was exfiltrated. It can state what the evidence shows—for example, that a user account uploaded a specified volume of data to an external destination—and identify what remains unknown.

The customer then evaluates the facts against its contractual, legal, and reporting obligations.

J.20 Lost or Stolen Device

A lost or stolen device incident requires identification of the device, assigned user, encryption state, authentication controls, management connectivity, last known activity, information potentially stored locally, and remote-protection capabilities.

Remote lock or wipe can be appropriate when authorized, but the team should consider evidence and reporting needs. The incident record should show what protections were active at the time of loss rather than relying on the intended configuration.

J.21 Cloud Incident

Cloud incidents can involve compromised identities, malicious application consent, exposed storage, suspicious mailbox rules, privileged-role changes, data sharing, or administrative misuse. Investigation should consider both human and non-human identities.

Party IJK should preserve cloud audit and identity records quickly because retention varies by service and licensing. Containment may require session revocation, role removal, application disablement, key rotation, or sharing restrictions.

J.22 RMM or MSP Platform Compromise

Compromise of an MSP management platform creates concentrated risk because one provider identity or tool may reach multiple customers. Party IJK should activate a provider-level incident process and separately determine the impact to each customer.

The MSP should not assume that because the RMM platform was compromised, every customer was affected. Nor should it assume customers were unaffected merely because no alert fired. Investigation should determine which tenants, devices, scripts, credentials, sessions, or actions were actually exposed.

Party ABC and Party EGH should receive customer-specific facts. Cross-customer information should remain separated.

J.23 Multi-Customer Incident Coordination

A multi-customer incident requires a provider command structure plus customer-specific workstreams. Party IJK may have one central technical investigation while maintaining separate incident records, evidence packages, communications, and impact determinations for Party ABC and Party EGH.

This separation is essential for confidentiality and assessment evidence. One customer's incident record should not contain another customer's CUI, architecture, credentials, or unrelated forensic details.

J.24 SIEM or Logging Failure During an Incident

Loss of a log source during an incident is both an operational problem and an investigative limitation. Party IJK should restore collection where possible, preserve locally available logs, identify the gap period, and document what evidence may be unavailable.

The incident team should not silently infer that no malicious activity occurred during the visibility gap. Conclusions should reflect the limitations of available evidence.

J.25 Third-Party and External Service Provider Incidents

A cloud, SOC, backup, identity, or other external provider may detect or experience an incident affecting the customer. Party IJK should capture the provider notification, identify affected services, determine customer-specific exposure, and coordinate technical actions.

Responsibility boundaries still apply. Provider statements should be preserved as source information, while the customer and MSP determine what those statements mean for the customer's environment and obligations.

J.26 Eradication

Eradication removes attacker persistence, malicious software, unauthorized accounts, unsafe configurations, exposed secrets, or other root causes. It should follow sufficient investigation to avoid removing the most visible symptom while leaving the actual access path intact.

Actions may include removing persistence, rebuilding systems, patching exploited vulnerabilities, rotating credentials, revoking tokens, correcting firewall rules, removing malicious applications, or changing architecture. Each action should be documented and validated.

J.27 Recovery

Recovery returns systems to trusted operation. The team restores services in a controlled sequence, monitors for recurrence, validates security tooling, confirms logging, checks identity state, and verifies business functionality.

Recovery should have explicit acceptance criteria. “Server is online” does not prove the system is safe, monitored, patched, backed up, and ready for normal use.

J.28 Recovery From Backup

Before restoring, the team should identify a recovery point that is appropriate for the incident and verify that backup infrastructure itself is trustworthy. Restored systems should receive required security updates, credential changes, monitoring, and validation before broad reconnection.

A restore test performed before an incident can dramatically reduce uncertainty. Incident response and backup readiness are therefore closely connected.

J.29 Communications During an Incident

Incident communications should be accurate, audience-specific, and controlled. Technical teams need operational facts. Executives need impact, decisions, and risk. Customers need information relevant to their environment. Contractual or legal reporting may require specific content and timing.

The incident lead should distinguish confirmed facts, working hypotheses, and unknowns. Speculation can create unnecessary confusion and may later conflict with evidence.

J.30 External Reporting and the MSP's Role

When DFARS 252.204-7012 applies, the contractor has the reporting obligation described by the clause. Party IJK can assist by rapidly providing the technical facts needed for the customer's review and report, but the service agreement should clearly identify whether the MSP has any delegated reporting role.

The clause's 72-hour period makes preparation important. Contact information, reporting access, required certificates or credentials, and internal decision authority should not be discovered for the first time during an incident.

J.31 Malicious Software Submission Considerations

DFARS 252.204-7012 also contains requirements concerning malicious software discovered and isolated in connection with a reported cyber incident. The clause directs submission to the DoD Cyber Crime Center according to applicable instructions rather than sending malicious software to the contracting officer.

The MSP should preserve the sample appropriately and coordinate with the contractor's reporting process rather than emailing potentially malicious files through ordinary channels.

J.32 Documentation and Ticket Quality

The incident record should show what was known, what was done, by whom, when, under whose authority, and with what result. Routine ticket shorthand is usually insufficient for a significant security incident.

Documentation should include the initial observation, severity changes, affected systems and identities, evidence references, containment, customer decisions, communications, eradication, recovery, validation, and unresolved actions. Sensitive evidence can be stored separately with references in the incident record.

J.33 Root Cause and Contributing Factors

Root-cause analysis should distinguish the initial access or failure mechanism from contributing conditions. A phishing message may initiate compromise, while excessive privilege, weak segmentation, or insufficient logging may increase impact.

The purpose is improvement, not blame. Corrective action should address both the immediate cause and material conditions that allowed the incident to progress.

J.34 Lessons Learned

After recovery, the team should review detection, escalation, authority, containment, evidence, communications, recovery, and customer coordination. The discussion should identify what worked and what needs improvement.

Lessons learned should produce assigned actions. A meeting that concludes “communication needs improvement” without changing contacts, procedures, tooling, or training does not strengthen the response capability.

J.35 Corrective Actions and Remediation

Post-incident actions may include technical remediation, policy changes, training, architecture changes, logging improvements, backup changes, access reviews, vendor changes, or updates to the incident plan.

Where a corrective action affects CMMC implementation or an existing remediation plan, the customer should connect the incident action to the appropriate governance record. Closing the incident ticket should not erase longer-term remediation work.

J.36 Testing the Incident Response Capability

The official CMMC Level 2 Assessment Guide expects organizations to test their incident response capability. Tabletop exercises can test decision-making and communication, while technical exercises can test isolation, evidence collection, restoration, and tooling.

Exercises should involve the people who would actually participate, including customer management and relevant business functions where appropriate. The after-action record should show improvements resulting from the test.

J.37 Party ABC Scenario: EDR Alert to Controlled Closure

Party IJK's SOC receives a high-severity EDR alert from a Party ABC engineering workstation. The analyst records the alert, device, user, timestamp, process chain, and network activity. Because the endpoint may contain CUI and the behavior suggests credential theft, the SOC escalates under ABC's incident matrix.

Party IJK is authorized to isolate endpoints under defined high-severity conditions, so the analyst isolates the workstation and preserves relevant EDR telemetry. ABC's security lead is notified through the approved channel. Investigation identifies a malicious attachment and suspicious authentication activity from the user's account.

The account is contained, sessions revoked, and related systems reviewed. Evidence indicates no observed lateral movement, but the team documents the scope and limitations of that conclusion. ABC evaluates contractual reporting requirements using the technical findings. Party IJK performs authorized eradication and recovery, validates endpoint security and identity state, and returns the device to service only after ABC's acceptance.

The incident closes with a timeline, evidence index, root-cause analysis, and corrective actions addressing email filtering and user awareness.

J.38 Party IJK Scenario: Compromised MSP Privileged Identity

Party IJK detects anomalous authentication involving a technician account with access to both Party ABC and Party EGH. Because the account creates multi-customer risk, Party IJK activates its provider incident process, disables the identity, revokes sessions, preserves authentication and RMM logs, and identifies actions performed by the account.

Separate customer workstreams are created. Evidence shows an attempted connection to an ABC device that was blocked and a successful administrative session to an EGH server. ABC and EGH receive different factual notifications reflecting their respective evidence.

The EGH workstream investigates commands, system changes, data access, and related identities. ABC's workstream validates the blocked attempt and searches for other access paths. Party IJK rotates relevant provider secrets and reviews other technician accounts.

This scenario demonstrates why MSP incidents require both centralized investigation and strict customer-specific evidence separation.

J.39 Party EGH Scenario: Ransomware Begins on a File Server

Party EGH reports inaccessible files while Party IJK's monitoring shows rapid file changes on a server. The service desk escalates immediately. The incident lead coordinates containment of the server and related identities while the backup team protects administrative access to recovery infrastructure.

The team identifies the likely initial compromised account and reviews authentication and endpoint evidence. Additional systems are checked for similar activity. Recovery

does not begin until the team addresses the access path and confirms a suitable clean backup point.

EGH management makes business and reporting decisions. Party IJK provides technical findings, restores the server under authorization, validates security controls and monitoring, and increases observation during the recovery period.

J.40 Closing Standard

An incident is not complete merely because the alert disappeared or the system came back online. Closure requires that containment is stable, eradication is validated, recovery is accepted, evidence is preserved, required communications are completed, unresolved risks are assigned, and lessons learned have been converted into actions.

For an MSP, closure also requires clear customer-specific documentation. Party IJK should be able to explain what it observed, what it did, what the customer decided, what evidence supports the conclusion, and what remains to be improved.

J.41 Incident Severity Matrix

Severity	Typical Characteristics	Response Expectation
Low	Suspicious event with limited impact; blocked or contained; no indication of sensitive-data exposure	Document, validate, monitor, close or escalate if facts change.
Moderate	Confirmed security incident with limited scope or privilege; manageable operational impact	Activate coordinated investigation; customer notification per plan; preserve evidence.
High	Privileged identity, sensitive system, possible CUI exposure, lateral movement, major outage, or active attacker	Immediate incident command, containment, executive/customer escalation, reporting evaluation.
Critical	Widespread compromise, ransomware, MSP platform compromise, material CUI exposure concern, severe operational disruption	Full incident command; multi-team response; executive/legal/contractual coordination; continuous tracking.

J.42 Incident Responsibility Matrix

Activity	Party IJK MSP/SOC	Customer ABC/EGH	Other Provider/Counsel
Detection and technical triage	Operate within service scope	Receive/escalate internal reports	Provide provider alerts as applicable

Containment	Execute pre-authorized actions; request approval otherwise	Authorize business-impacting actions	Support provider-specific containment
Evidence preservation	Preserve MSP-held technical evidence	Preserve customer-held records and direct organizational preservation	Preserve provider evidence
Contractual reporting decision	Provide technical facts	Own decision/obligation unless formally delegated and permitted	Advise/support as authorized
Recovery	Execute technical restoration/validation	Approve return to service	Support dependent services
Lessons learned	Provide technical findings and MSP actions	Own organizational corrective actions	Participate where relevant

J.43 Incident Intake Checklist

- Customer and reporter identified.
- Date/time/time zone recorded.
- Affected asset, identity, service, or location recorded.
- Detection source and original alert preserved.
- Observed symptoms recorded without unsupported conclusions.
- Potential business/CUI relevance noted.
- Immediate safety/continuity impact identified.
- Incident contact and escalation path activated as required.

J.44 Triage and Containment Checklist

- Determine whether activity is ongoing.
- Identify privilege level and potential scope.
- Check for related alerts, identities, systems, and network activity.
- Assign initial severity and record rationale.
- Preserve relevant logs and telemetry.
- Confirm containment authority.
- Isolate systems or restrict identities when authorized and appropriate.
- Document every containment action and validation.
- Reassess severity after new evidence.

J.45 Evidence Preservation Checklist

- Preserve original alerts and relevant log records.
- Record system clocks/time zones and collection times.
- Preserve endpoint/cloud/identity/network telemetry relevant to the incident.
- Protect collected evidence from unauthorized modification.
- Record who collected or exported important artifacts.
- Avoid unnecessary reboot, reimage, deletion, or log clearing before preservation decisions.
- Identify DFARS media-preservation obligations when applicable.
- Maintain customer separation for MSP-held evidence.

J.46 Recovery Validation Checklist

- Initial access/persistence path addressed.
- Compromised credentials/tokens/keys rotated or revoked as required.
- Required patches or configuration corrections applied.
- Endpoint and identity security controls healthy.
- Logging/SIEM ingestion restored and validated.
- Backup/recovery state validated.
- Business application functionality tested.
- Heightened monitoring period established where appropriate.
- Customer acceptance to return to service recorded.

J.47 Incident Chronology Template

Time/Zone	Actor	Observation or Action	Authority/Decision	Evidence Reference
	SOC/Technician			
	Incident Lead			
	Customer			
	Recovery Team			

J.48 Incident Evidence Index Template

Evidence ID	Artifact	Source	Collected	Storage/	Customer

			By/When	Integrity Note	Relevance
EV-001	Original alert				
EV-002	Authentication logs				
EV-003	Endpoint telemetry				
EV-004	Incident ticket/timeline				

J.49 Lessons-Learned and Corrective-Action Template

Finding	Why It Mattered	Corrective Action	Owner	Target Date	Closure Evidence

J.50 Authoritative Sources for This Teaching Edition

The regulatory and CMMC-specific statements in this teaching edition were checked against current official sources on September 22, 2026. Because CMMC implementation is under review, all time-sensitive program statements should be reverified before final publication or use on a specific contract.

- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024), Acquisition.gov.
- CMMC Assessment Guide – Level 2, Version 2.13, Department CMMC program resources.
- Current CMMC About and Resources & Documentation pages, Department CMMC program, verified September 22, 2026.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program.

Deepening Pass — The First 15 Minutes

The first fifteen minutes should create control, not perfect understanding. The person receiving the alert confirms the customer, preserves the original notification, records

the time and time zone, identifies the affected asset or identity, and determines whether harmful activity appears to be continuing. If a pre-authorized emergency containment action is clearly warranted, it is taken and documented.

The technician should avoid turning triage into uncontrolled troubleshooting. Rebooting, deleting files, running broad cleanup tools, or resetting multiple accounts can change the evidence before the incident lead understands the situation.

The first escalation message should separate confirmed facts from suspicion. For example: “EDR detected credential-dumping behavior on workstation ABC-ENG-014 at 10:42 Eastern; the workstation is isolated under ABC's approved high-severity containment authority; investigation is continuing.” This is more useful than stating that ABC “has been breached” before the facts support that conclusion.

Deepening Pass — Minutes 15–60: Establishing Incident Command

During the next phase, the incident lead establishes a working scope, severity, customer decision contact, technical assignments, evidence location, and communication cadence. The team identifies what must happen immediately and what should wait until evidence is preserved.

Analysts search for related identities, endpoints, IP addresses, processes, domains, cloud events, or administrative activity. The objective is to determine whether the first alert represents one affected asset or part of a larger pattern.

The incident lead also identifies business constraints. Is the affected system a production server? Does isolation stop manufacturing? Is an executive account involved? Does the system process or store CUI? These facts influence containment and escalation without changing the requirement to document what is actually known.

Deepening Pass — Hours 1–4: Containment and Scope Expansion

Once incident command is stable, the team moves from initial containment to deliberate scope analysis. Endpoint, identity, cloud, network, RMM, SIEM, firewall, and application evidence may be correlated. The team should look for evidence of initial access, privilege escalation, persistence, lateral movement, command and control, collection, or data transfer as relevant to the event.

Containment decisions should be recorded with the reason for each action. If Party ABC decides not to isolate a production server immediately because of a safety or

operational dependency, that decision and compensating measures should be documented.

The team should continually revisit the question: “What evidence would change our current scope?” This guards against premature closure around the first affected device.

Deepening Pass — The First 24 Hours

Within the first day, a significant incident should have a reliable chronology, known affected assets and identities, a current containment state, preserved key evidence, assigned decision-makers, and a documented list of unknowns. Recovery planning may begin, but it should not outrun investigation.

Party IJK should prepare a concise customer status package containing confirmed facts, current impact, containment completed, evidence preserved, actions in progress, decisions required, and unresolved questions. The package should avoid unsupported attribution or claims about data exposure.

If contractual reporting may apply, the customer should already be evaluating the incident against the applicable clause rather than waiting for the technical investigation to become perfect.

Deepening Pass — Supporting the 72-Hour DFARS Reporting Window

When DFARS 252.204-7012 applies, the contractor's rapid-reporting requirement makes early information discipline essential. The MSP should organize technical facts so the customer can make its reporting determination and prepare the required submission without waiting for a complete forensic report.

The technical support package should identify the discovery time, affected systems, known or suspected compromise, covered information potentially involved, containment status, relevant indicators, and what remains under investigation. The MSP should update the customer as material facts change.

The 72-hour requirement is not a reason to speculate. A timely report can reflect information known at the time and can be supplemented as investigation develops according to the applicable process. Party IJK's role is to accelerate reliable fact production and preservation.

Deepening Pass — Evidence Handling and Chain of Custody

For incidents that may require deeper investigation, the team should record who collected an artifact, when it was collected, the source system, collection method, where it was stored, and any integrity information generated by the collection process. Access to evidence should be restricted to personnel who need it.

Not every incident requires formal forensic imaging of every system. The response plan should scale evidence handling to incident significance, contractual requirements, investigative needs, and available expertise.

When outside forensic specialists are engaged, Party IJK should preserve the existing evidence and avoid unnecessary changes while coordinating transfer. The MSP's ticket should reference evidence locations rather than embedding highly sensitive artifacts indiscriminately.

Deepening Pass — Ransomware: Detailed Operational Sequence

A ransomware incident can evolve faster than ordinary ticket escalation. The first objective is to limit spread while protecting the ability to investigate and recover. Party IJK identifies active encryption, affected hosts, implicated identities, reachable file shares, remote-management activity, and backup exposure.

The identity team reviews privileged and service accounts and may revoke sessions or disable compromised credentials under approved authority. The network and endpoint teams isolate affected systems or segments as appropriate. The backup team protects backup administration and verifies that recovery repositories have not been altered.

Investigation then seeks the initial access path and persistence. Recovery begins from a trusted point only after the team has addressed the mechanism that would allow the attacker to return. Restored systems are patched, monitored, and validated before normal access resumes.

Party IJK documents technical facts. Party EGH management handles organizational decisions regarding business interruption, insurer contact, legal counsel, contractual reporting, law enforcement, and any ransom-related matter.

Deepening Pass — RMM Compromise: Provider-Level Emergency Workflow

An RMM compromise should be treated as a potential provider-wide incident because the platform may provide administrative reach into many customers. Party IJK first protects the management plane: affected provider identities are disabled, sessions revoked, API tokens reviewed, automation suspended where appropriate, and platform/vendor support engaged.

The investigation identifies which customer tenants, endpoints, scripts, commands, file transfers, or credentials were touched. Customer impact should be determined from evidence rather than assumed from platform-wide exposure.

Party IJK establishes separate customer records. Party ABC receives facts about ABC; Party EGH receives facts about EGH. A central provider investigation can reference customer-specific evidence without combining sensitive customer information into a shared notification.

Recovery requires confidence in the RMM control plane, provider identities, API integrations, scripts, and technician endpoints before broad remote administration resumes.

Deepening Pass — Compromised MSP Administrator

A compromised MSP administrator is both an identity incident and a trust-boundary incident. The response team should identify every customer and provider system the account could reach, then distinguish theoretical access from observed activity.

The account is contained, active sessions and tokens are revoked, authentication methods reviewed, and related privileged credentials assessed. Logs from identity, RMM, VPN, cloud, PSA, vault, and customer systems can help reconstruct activity.

If the account accessed Party EGH but only attempted and failed to reach Party ABC, those customers require different incident narratives. Accurate customer-specific communication is preferable to a broad statement that all customers were compromised.

Deepening Pass — Communications Tree

The communications tree should identify technical escalation, customer operational contact, customer executive contact, security leadership, legal/contractual contacts

where applicable, insurer or outside forensics contacts, and relevant service providers. After-hours alternatives should be tested.

Communication channels should be chosen with the incident in mind. If email compromise is suspected, the team should use an approved alternate channel. If the MSP's own collaboration environment is compromised, customer communications may need a separate trusted method.

Every significant external communication should have an owner. Multiple technicians independently calling the customer can create contradictory information and distract responders.

Deepening Pass — Executive Situation Report

An executive situation report should be short enough to read quickly but precise enough to support decisions. It should state the incident status, confirmed impact, affected business services, containment state, significant unknowns, decisions required, and next update time.

Technical indicators and detailed forensic observations can be attached or maintained separately. Executives usually need to know what the organization must decide, not every process name seen in EDR.

The report should label uncertainty explicitly. “No evidence observed to date” is different from “did not occur,” particularly when logging gaps exist.

Deepening Pass — Customer Status Update Example

At 14:00 Eastern, Party IJK reports to Party ABC: one engineering workstation remains isolated; the user's sessions have been revoked; EDR and identity logs show suspicious credential activity; no confirmed lateral movement has been identified in the evidence reviewed so far; investigation of cloud authentication and adjacent engineering systems continues; no recovery action has yet been authorized.

This update is useful because it distinguishes containment, evidence, current conclusion, limitations, and next work. It does not promise that the investigation is complete.

Deepening Pass — Recovery Decision Gate

Before recovery, the incident lead should ask whether the initial access path is understood sufficiently, persistence has been addressed, compromised credentials are

controlled, required evidence is preserved, the recovery source is trustworthy, and monitoring is ready to detect recurrence.

If the answer to a critical question is no, the team should document why recovery is nevertheless necessary or delay recovery until the condition is addressed.

The customer should approve restoration of materially affected business services according to its incident plan. Party IJK then executes the technical recovery and documents validation.

Deepening Pass — Heightened Monitoring After Recovery

Recovery should be followed by a defined heightened-monitoring period. Party IJK may increase review of identity events, endpoint detections, network connections, newly created accounts, privileged changes, or indicators associated with the incident.

The duration should reflect the incident rather than follow an arbitrary universal number. The closure record should state what was monitored, for how long, and whether suspicious recurrence was observed.

This period provides evidence that recovery remained stable rather than ending response at the moment a system came back online.

Deepening Pass — Tabletop Exercise: Compromised RMM Technician Account

A useful MSP tabletop begins with a high-risk login to a Party IJK technician account. Ten minutes later, an RMM script runs against Party EGH. Party ABC then reports an unexpected remote-support prompt. The exercise participants must decide how to contain the provider identity, how to determine customer impact, how to communicate separately with each customer, and how to preserve provider and customer evidence.

The facilitator introduces complications: the primary incident contact at EGH does not answer; Party ABC asks whether CUI was accessed; the RMM vendor reports a service issue; and the technician whose account is involved is traveling.

The exercise should evaluate authority, communications, customer separation, evidence, and decision quality—not merely whether participants name the right security tools.

Deepening Pass — Tabletop Exercise: Ransomware and Backup Uncertainty

In a second exercise, Party EGH's file server begins encrypting data. The last documented restore test was six months ago. The backup console shows successful jobs, but a privileged backup account authenticated from an unusual location earlier that morning.

Participants must decide how to protect backup infrastructure, what to isolate, which evidence to preserve, when recovery can safely begin, and how management receives status. The facilitator can reveal additional facts gradually to test whether the team revises severity and scope appropriately.

The after-action review should produce concrete improvements to contacts, backup validation, privilege separation, or procedures.

Deepening Pass — Incident Metrics That Matter

Useful incident metrics should improve readiness rather than reward superficial speed. Measures can include time from detection to triage, time to appropriate escalation, time to containment, percentage of incidents with complete timelines, evidence-preservation quality, recurrence, overdue corrective actions, and exercise findings closed.

A low mean time to close can be misleading if incidents are closed before root causes or corrective actions are addressed. Metrics should encourage reliable response and learning.

Deepening Pass — Post-Incident Evidence Package

The final evidence package should allow an authorized reviewer to reconstruct the response without searching across dozens of systems. It can include the incident summary, chronology, severity history, affected-asset list, evidence index, containment record, customer decisions, reporting references, eradication and recovery validation, communications record, root-cause analysis, lessons learned, and corrective-action register.

Sensitive raw evidence can remain in protected repositories and be referenced by identifier. The package should preserve customer separation and follow applicable retention requirements.

Deepening Pass — First-Hour Field Checklist

- Preserve the original alert/report and record discovery time and time zone.
- Confirm customer, affected asset/identity, and immediate operational impact.
- Determine whether harmful activity appears active.
- Apply only pre-authorized emergency containment; document action and authority.
- Assign incident lead and initial severity.
- Activate customer escalation and alternate communications if needed.
- Preserve priority endpoint, identity, cloud, network, and management-platform evidence.
- Search for related assets, identities, indicators, or administrative actions.
- Establish incident timeline and evidence repository.
- Identify decisions requiring customer management.
- Set the next status-update time.

Deepening Pass — 72-Hour Reporting Support Checklist

- Confirm whether the customer is evaluating the incident under DFARS 252.204-7012 or another applicable requirement.
- Record precise discovery time used by the customer for its process.
- Provide customer-specific affected-system and identity facts.
- Identify covered information potentially involved without overstating conclusions.
- Provide known indicators, containment actions, and current scope.
- Identify significant unknowns and evidence limitations.
- Preserve relevant media/logging in accordance with applicable requirements.
- Maintain an update process as material facts change.
- Reference customer reporting confirmation in the incident record without exposing unnecessary credentials or sensitive submission data.

Substantive Pass — Incident Command Structure for an MSP

A mature MSP should distinguish incident command from technical specialization. The incident lead coordinates priorities, customer decisions, assignments, communications, evidence, and the operational picture. Endpoint, identity, cloud, network, backup, and forensic specialists may each lead their technical workstreams, but they should report into one coordinated incident process.

For a customer incident, Party ABC or Party EGH should identify an organizational decision authority. Party IJK can direct technical work that is within its delegated authority, but it should not silently convert technical control into authority over contractual reporting, business shutdown, public communications, legal decisions, or organizational risk acceptance.

For a provider-level incident, Party IJK may also need an internal executive lead because decisions affecting multiple customers, provider infrastructure, employee access, vendor engagement, and business continuity extend beyond a single customer ticket.

Substantive Pass — Decision Authority Under Pressure

The incident plan should identify decisions that technicians can make immediately and decisions that require customer or management authorization. Pre-authorization is especially important for endpoint isolation, account disablement, session revocation, firewall blocking, emergency change, and removal of malicious persistence.

The plan should also address exceptions. If isolating a production system could stop manufacturing or create a safety concern, the technician needs a rapid path to the authorized customer decision-maker. The record should show the requested action, the risk of delay, the decision, and any compensating containment.

This structure protects speed without encouraging unauthorized action. Incident response becomes faster when authority has been designed in advance.

Substantive Pass — Evidence Acquisition Strategy

Evidence acquisition should answer investigative questions rather than become indiscriminate collection. The team should identify what it needs to establish: initial access, affected identity, execution, persistence, privilege escalation, lateral movement, data access, transfer, or recovery state.

For an endpoint incident, evidence may include EDR telemetry, relevant event logs, process execution, network connections, persistence locations, authentication events, and selected forensic artifacts. For a cloud incident, audit records, identity events, role changes, application consent, mailbox or file activity, and session information may be more important.

The collection plan should record source, collector, time, method, storage location, and integrity information where appropriate. When specialized forensic acquisition is needed, Party IJK should engage qualified resources rather than improvising beyond its capability.

Substantive Pass — Suspected CUI Exfiltration Investigation

A suspected CUI exfiltration event requires disciplined language and evidence. The investigation should first identify the information repository, affected account or system, destination, transfer mechanism, time range, file or object activity, and relevant network or cloud telemetry.

The team should distinguish access, staging, attempted transfer, successful transfer, and confirmed receipt by an unauthorized destination. These are different facts. A large outbound connection can be suspicious without proving that CUI was exfiltrated.

Party IJK should provide Party ABC with the strongest supportable technical statement and the limitations of the evidence. ABC can then evaluate the facts against its contractual and organizational reporting process. If additional evidence later changes the conclusion, the incident record should preserve that evolution.

Substantive Pass — Cloud Identity and Application-Consent Compromise

Modern cloud compromise may persist without a stolen password. An attacker may obtain a session token, register a new authentication method, create an inbox rule, obtain application consent, add a service principal credential, or assign a privileged role.

The response therefore should inspect more than sign-in failures. Party IJK should examine successful authentication, token/session activity where available, MFA changes, registered devices, privileged-role changes, application consent, service principals, mailbox or collaboration changes, and unusual sharing.

Containment can require session revocation, password reset, MFA re-registration, removal of malicious authentication methods, revocation of application consent, secret rotation, or role removal. Recovery should verify that the identity and associated applications have returned to the approved state.

Substantive Pass — Insider Activity and Authorized-User Misuse

Not every incident involves an external attacker. Suspicious copying, unauthorized cloud sharing, use of removable media, deliberate policy bypass, or misuse of privileged access can involve an otherwise valid user.

Party IJK should avoid making employment or intent judgments. It should preserve technical facts and follow the customer's escalation process. Investigation may require tighter confidentiality because broad notification could compromise the inquiry.

Customer management, human resources, legal counsel, or other authorized functions may direct how the matter is handled. The MSP's role remains technical unless its contract assigns additional responsibilities.

Substantive Pass — Third-Party Provider Compromise

When a cloud provider, SOC, backup provider, software vendor, or other external service reports compromise, Party IJK should translate the provider's notification into customer-specific questions. Which services are used by Party ABC? Which identities or integrations connect to them? What customer data or security functions depend on the provider? What compensating actions are available?

Provider statements should be preserved, including updates that change earlier conclusions. Party IJK should not simply forward a vendor bulletin and close the ticket. It should determine whether the customer's environment requires action.

If the affected provider is itself a security protection asset or supports a security requirement, the incident may also create an evidence and readiness issue even when no CUI exposure is identified.

Substantive Pass — Business Continuity During Containment

Containment and business continuity can conflict. Disabling a domain account may interrupt production automation; isolating a server may stop order processing; blocking a cloud service may prevent employees from working.

The incident lead should present decision-makers with technically realistic options. For example, a system might be segmented rather than powered off, a privileged account might be restricted rather than deleted, or a service might be restored in a clean isolated environment.

The response record should document the risk accepted when containment is delayed or modified for business reasons. This is not evidence of weak response if the decision is informed, authorized, and supported by compensating controls.

Substantive Pass — Full Incident Record Example: Party ABC

At 10:42 Eastern, Party IJK's SOC receives an EDR alert from ABC-ENG-014 indicating credential-dumping behavior. The analyst confirms that the endpoint is assigned to an engineer working with controlled technical information. At 10:47, the endpoint is isolated under ABC's pre-approved high-severity containment rule. The original alert, process tree, network telemetry, and relevant endpoint events are preserved.

At 10:55, the incident lead is assigned and ABC's security lead is notified. Identity review identifies an unusual successful authentication by the engineer's account at 10:31 and a new session from an unfamiliar source. Sessions are revoked and the account is temporarily disabled under ABC's approved identity-containment procedure.

By 11:35, investigation finds a malicious attachment opened shortly before the endpoint behavior. No confirmed lateral movement has been identified in the logs reviewed, but the team explicitly records that investigation is continuing. Adjacent engineering systems and cloud authentication are examined.

At 13:20, Party IJK provides ABC with a status report distinguishing confirmed compromise of the workstation and account from the still-unresolved question of data exposure. ABC begins its contractual reporting evaluation using Party IJK's technical package.

After evidence preservation, Party IJK rebuilds the endpoint from the approved baseline, rotates affected credentials, validates EDR and logging, and confirms required applications. ABC authorizes return to service after heightened monitoring is established. The final record contains the chronology, evidence index, containment decisions, recovery validation, ABC reporting reference, root cause, and corrective actions.

Substantive Pass — Full Incident Record Example: Party IJK RMM Compromise

At 02:14 Eastern, Party IJK's identity platform detects an anomalous privileged login by a technician account. At 02:19, the account initiates an RMM script against several managed endpoints. The provider incident process is activated, the identity is disabled, sessions revoked, and relevant RMM automation paused.

Party IJK preserves identity, RMM, vault, VPN, PSA, and technician-endpoint evidence. A customer-impact matrix is created. Logs show successful script execution on two Party EGH endpoints, a blocked connection attempt to one Party ABC endpoint, and no observed activity for other customers in the reviewed time range.

Party IJK creates separate customer workstreams. EGH receives details of the executed commands and affected devices. ABC receives information about the blocked attempt and the additional validation being performed. Neither customer receives the other's environment details.

The investigation identifies credential theft from the technician workstation. Party IJK isolates and rebuilds the technician device, rotates relevant provider credentials, reviews other privileged identities, validates RMM API integrations, and coordinates with the RMM vendor. Customer environments receive targeted validation before routine RMM administration resumes.

The after-action review results in stronger technician workstation controls, revised RMM emergency procedures, tighter privileged-session monitoring, and a recurring review of provider API tokens.

Substantive Pass — Full Incident Record Example: Party EGH Ransomware

At 07:18 Eastern, EGH employees report that files on a shared server are being renamed and cannot be opened. Party IJK monitoring simultaneously detects rapid file changes. The incident is classified high and escalated. The file server is isolated according to the approved emergency procedure, and suspicious user sessions are revoked.

The backup team protects backup administrative access before initiating restoration. Review shows an unusual privileged backup login earlier in the morning, so the team

treats backup integrity as uncertain until validated. Identity and endpoint investigation identifies a compromised account and evidence of remote execution from a workstation.

The affected workstation is isolated. The compromised identity is disabled and sessions revoked. Additional servers are checked for related activity. Party IJK preserves the relevant evidence and provides EGH management with confirmed facts and unknowns.

A clean recovery point is identified and tested in an isolated recovery environment. Only after the initial access path and affected credentials are addressed does EGH authorize production restoration. The restored server receives security updates, EDR validation, logging validation, and heightened monitoring before users reconnect.

Substantive Pass — After-Action Report Structure

The after-action report should begin with an executive summary that explains what happened, the business impact, and the final status without excessive technical detail. A technical chronology then reconstructs the incident from earliest known activity through closure.

The report should identify affected assets and identities, evidence sources, containment and eradication actions, recovery validation, significant decisions, communications, contractual reporting references where applicable, root cause, contributing factors, and evidence limitations.

The final section should contain corrective actions with owners and target dates. The report should distinguish actions already completed from longer-term remediation so that closure of the incident does not close the improvement program.

Substantive Pass — Assessment-Ready Incident Response Evidence

For CMMC readiness, the organization should be able to show that incident response is operational rather than theoretical. Evidence can include the incident response plan, roles, contact lists, training, tabletop exercises, actual incident records, incident tracking, reporting procedures, lessons learned, and corrective actions.

The assessor may examine records, interview personnel, and test whether the process is understood and implemented. A well-maintained incident package helps personnel explain the process consistently because it reflects real operations.

Party IJK should provide customer-specific evidence for the services it performs while protecting other customers and provider-sensitive information. The customer's SSP and responsibility documentation should explain how MSP incident-response services fit into the organization's implementation.

Substantive Pass — Incident Response Evidence Retention

Incident records should have a defined retention approach that accounts for contractual obligations, organizational policy, legal needs, security investigations, and the usefulness of historical evidence for assessment. Raw telemetry may have a different retention period from final incident reports or corrective-action records.

The MSP should understand which records belong to the customer, which are provider operational records, and which contain multi-customer or provider-sensitive information. Offboarding should not inadvertently eliminate evidence the customer reasonably needs to demonstrate historical incident handling.

Where DFARS 252.204-7012 media-preservation requirements apply to a reported cyber incident, the specific preservation requirement should be followed in addition to ordinary incident-record retention.

Substantive Pass — When to Engage Specialized Forensics

Some incidents exceed ordinary MSP investigation. Indicators include destructive attacks, suspected significant CUI exfiltration, sophisticated persistence, compromise of domain or cloud control planes, litigation concerns, law-enforcement involvement, or a need for forensic conclusions beyond the MSP's expertise.

The incident plan should identify how specialized forensics is engaged and who authorizes it. Party IJK should preserve the environment and evidence so the specialist receives the best possible starting point.

Recognizing the boundary of MSP expertise is a strength. Overconfident amateur forensics can destroy evidence and create unsupported conclusions.

Substantive Pass — Incident Closure Gate

Closure should be a decision gate rather than a technician changing a ticket status. The incident lead confirms that active threat is contained, eradication is validated, recovery is accepted, required evidence is preserved, customer communications are

complete, reporting references are recorded where applicable, and longer-term actions have owners.

The customer should acknowledge closure for significant customer incidents. Party IJK should separately close any provider-level corrective actions that remain from an MSP-caused or MSP-platform incident.

A reopened incident should preserve the original chronology and explain why new evidence changed the closure decision.

Substantive Pass — Incident Command Decision Checklist

- Assign one incident lead and one customer organizational decision contact.
- Confirm technician pre-authorizations and actions requiring additional approval.
- Establish severity, scope hypothesis, communication cadence, and evidence repository.
- Identify business-continuity constraints before disruptive containment.
- Separate confirmed facts, hypotheses, and unknowns in every major update.
- Maintain customer-specific records during multi-customer events.
- Record decisions to delay or modify containment and the compensating controls.
- Confirm reporting evaluation ownership and technical support responsibilities.
- Establish explicit recovery and closure decision gates.

Substantive Pass — Suspected CUI Exposure Investigation Checklist

- Identify the repository, files/objects, system, and responsible identity.
- Establish the relevant time range and preserve source telemetry.
- Determine whether evidence shows access, staging, attempted transfer, successful transfer, or confirmed unauthorized receipt.
- Identify destination, protocol/service, volume, and related authentication activity where available.
- Check for related cloud sharing, email, removable media, or third-party transfer mechanisms as relevant.
- Document evidence limitations and visibility gaps.
- Provide the customer with supportable technical facts without making unsupported contractual conclusions.
- Update the incident record when later evidence changes the working conclusion.

Substantive Pass — After-Action Report Checklist

- Executive summary and final incident status.
- Discovery time, chronology, and severity history.
- Affected assets, identities, services, and business impact.
- Evidence sources and significant limitations.
- Containment, eradication, and recovery actions.
- Customer and management decisions.
- Contractual reporting references where applicable.
- Root cause and contributing factors.
- Lessons learned and control/process improvements.
- Corrective actions with owners, target dates, and closure evidence.
- Incident closure approval.

Substantive Pass — Final Teaching Perspective

A strong incident response program is not defined by the number of security products an MSP operates. It is defined by whether the MSP and customer can recognize abnormal activity, establish command, preserve evidence, make authorized containment decisions, determine scope, communicate accurately, recover safely, meet applicable obligations, and learn from the event.

For Party IJK, the most important discipline is to combine technical speed with responsibility boundaries. The MSP should move quickly where it has authority, escalate quickly where it does not, and produce evidence that allows Party ABC or Party EGH to make informed organizational decisions. That combination of speed, evidence, and governance is what turns an incident-response document into an operational capability.

Final Regulatory Verification and Publication Note

This appendix is an operational incident-response guide for MSPs and their customers. It does not replace the contractor's incident response plan, System Security Plan, contractual requirements, legal advice, or reporting determinations. The applicable solicitation, contract, task order, delivery order, and flowdown clauses remain controlling.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024), defines “rapidly report” as within 72 hours of

discovery of a cyber incident. When the clause applies and the contractor discovers a cyber incident affecting a covered contractor information system, covered defense information residing therein, or designated operationally critical support, the clause requires the contractor to conduct the specified review and rapidly report the incident to DoD.

For a reported cyber incident, DFARS 252.204-7012 requires preservation and protection of images of all known affected information systems identified by the clause and relevant monitoring or packet-capture data for at least 90 days from submission of the cyber incident report. The clause also states that malicious software discovered and isolated in connection with a reported cyber incident is submitted to the DoD Cyber Crime Center according to applicable instructions and is not sent to the Contracting Officer.

The current CMMC Level 2 Assessment Guide, Version 2.13, addresses an operational incident-handling capability under IR.L2-3.6.1 and includes preparation, detection, analysis, containment, recovery, and user response activities. The guide describes examine, interview, and test assessment methods, reinforcing this appendix's emphasis on operational records, personnel understanding, exercises, and demonstrable incident-handling processes.

As verified September 22, 2026, current Department CMMC materials state that Phase II implementation, originally scheduled for November 10, 2026, was suspended on July 13, 2026; Phase I self-assessment requirements remain in place while the program is under review. Current Department materials also state that the pause does not eliminate the requirement to protect information in accordance with DFARS 252.204-7012. Readers should reverify current CMMC program guidance before applying this appendix to a specific procurement or assessment.

Authoritative Sources Used for Final Verification

- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024), Acquisition.gov.
- CMMC Assessment Guide – Level 2, Version 2.13, Department CMMC program resources.
- Current CMMC About and Resources & Documentation pages, Department CMMC program, verified September 22, 2026.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program.

Appendix K

CMMC / NIST SP 800-171 Cross-Reference

Detailed Teaching and Operational Edition

K.1 Purpose of This Cross-Reference

This appendix connects CMMC Level 2 to the 110 security requirements in NIST SP 800-171 Revision 2 in a way that is useful to an MSP, MSSP, defense contractor, readiness team, and assessor-facing technical staff. It is not intended to replace the official NIST publication or the current CMMC Assessment Guide. Its purpose is to help the reader understand how the requirements become operational work, evidence, responsibility assignments, and assessment activity.

A cross-reference is most useful when it answers more than “what control number is this?” For each family, the reader should understand the security outcome, typical MSP contribution, contractor responsibility, likely evidence, and how an assessor may examine, interview, or test the implementation.

K.2 Why Revision 2 Still Matters in the Current CMMC Context

NIST withdrew SP 800-171 Revision 2 in May 2024 after publishing Revision 3. However, current Department CMMC materials continue to identify the 110 requirements of NIST SP 800-171 Revision 2 as the Level 2 requirement set during the current Phase I implementation posture.

This distinction is important. An MSP may be designing future security improvements with newer NIST publications in mind, but it should not silently substitute Revision 3 requirements for the Revision 2 requirements used by the current CMMC Level 2 program materials. Contract language and current official CMMC guidance control the compliance basis.

K.3 CMMC Is an Assessment Framework, Not a Replacement for NIST SP 800-171

CMMC provides a framework for assessing contractor implementation of applicable cybersecurity protections. At Level 2, the current program materials point to the 110 NIST SP 800-171 Revision 2 requirements. The CMMC Assessment Guide then

provides assessment objectives and methods that help determine whether those requirements are satisfied.

The practical lesson is that the MSP should not build a separate “CMMC control environment” disconnected from ordinary security operations. The organization should implement the security requirements in its real environment and maintain evidence showing that the implementation works.

K.4 The Four-Layer Reading Method

A useful way to read any Level 2 requirement is through four layers. First is the NIST requirement: what security outcome must be achieved. Second is the assessment objective: what specific determinations must be made. Third is the operational implementation: what people, processes, technologies, and configurations actually accomplish the outcome. Fourth is the evidence: what demonstrates that the implementation exists and operates.

This four-layer method prevents a common mistake—treating a policy statement as if it were proof that a technical requirement is implemented.

K.5 Assessment Methods: Examine, Interview, and Test

The official CMMC Level 2 Assessment Guide uses the NIST SP 800-171A assessment approach. Examine means reviewing or analyzing specifications, mechanisms, and activities. Interview means discussing implementation with individuals or groups. Test means exercising mechanisms or activities under defined conditions and comparing actual behavior with expected behavior.

An MSP should therefore prepare for all three. A screenshot can support examine. A technician may be interviewed about account provisioning. An assessor may test whether an inactive session locks or whether an unauthorized user is denied access. Evidence preparation must reflect the real assessment method.

K.6 The Four Types of Assessment Objects

Assessment objects include specifications, mechanisms, activities, and individuals. Specifications are documents such as policies, procedures, security plans, requirements, and designs. Mechanisms are hardware, software, and firmware safeguards. Activities are protection-related actions such as backups or monitoring. Individuals are the people who implement or operate the safeguards.

For an MSP, this means the assessment may touch the customer's SSP, the MSP's service procedures, an EDR or identity configuration, actual monitoring tickets, and the technician who performs the work.

K.7 Responsibility Does Not Automatically Transfer to the MSP

A contractor can outsource technology and operational work without outsourcing its organizational accountability. Party IJK may operate identity, endpoint, logging, backup, vulnerability management, or incident-response services for Party ABC, but ABC still needs to understand how those services satisfy its requirements and how they are represented in its SSP and responsibility documentation.

The cross-reference therefore identifies typical MSP contributions rather than declaring that the MSP “owns” a NIST requirement. Actual responsibility depends on architecture, contract, service agreement, and implementation.

K.8 Evidence Should Be Requirement-Specific

A single policy or product dashboard rarely proves an entire family. Evidence should connect directly to the requirement and assessment objective. For access control, that may include account lists, group membership, access approvals, configuration, and demonstrations. For vulnerability remediation, it may include scan results, tickets, patch records, exception decisions, and rescans.

The strongest evidence often arises naturally from well-run operations rather than being manufactured immediately before assessment.

K.9 Family-Level Cross-Reference Overview

NIST SP 800-171 R2 Family	Reqs.	Security Outcome	Typical MSP Contribution	Typical Contractor Responsibility	Representative Evidence
3.1 Access Control (AC)	22	Limit system access to authorized users, processes acting on behalf of authorized users, and authorized devices; control functions, remote access, wireless access, mobile devices, and CUI flow.	Identity platforms, directory services, MFA, VPN, conditional access, firewall rules, endpoint/device controls, RMM permissions, access reviews, and ticketed provisioning.	Approved user/access policy, authorization decisions, business-role definitions, CUI flow decisions, exceptions, and periodic management review.	Account exports; group memberships; MFA/conditional-access configuration; VPN and firewall settings; access requests; termination tickets; privileged-access reviews; demonstrations of allowed and denied

					access.
3.2 Awareness and Training (AT)	3	Ensure managers, administrators, users, and security personnel understand security risks, responsibilities, and role-specific duties.	Provide technical-security training for MSP technicians, document platform procedures, support phishing/security awareness platforms, and maintain technician competency records.	Define required training, ensure personnel complete it, provide role-specific awareness, and retain organizational training evidence.	Training assignments and completion; role-based technician training; awareness communications; interview responses; exercise records.
3.3 Audit and Accountability (AU)	9	Create, protect, review, and retain audit records needed to monitor, investigate, and report inappropriate or unauthorized activity.	Configure logging, centralize events, synchronize time, operate SIEM/SOC, protect logs, investigate alerts, and support retention.	Determine audit needs and retention consistent with risk and requirements; ensure relevant systems are included; review provider service boundaries.	Logging configurations; SIEM source inventory; sample logs; alert tickets; time synchronization; retention settings; privileged audit access; review records.
3.4 Configuration Management (CM)	9	Establish and maintain system baselines, control changes, restrict unnecessary functionality, and manage software and configuration settings.	Build secure baselines, deploy configuration policies, manage patches/configurations, maintain RMM/MDM policies, document changes, and detect drift.	Approve baselines and business exceptions, define change authority, maintain system descriptions, and accept operational risk.	Baseline documents; configuration exports; change tickets; software inventory; prohibited software controls; exception approvals; before/after configuration evidence.
3.5 Identification and Authentication (IA)	11	Identify users, devices, and processes and authenticate identities before access, including multifactor authentication and password/authenticator protections.	Operate directory/identity platforms, MFA, privileged identity, service-account controls, certificate/device identity, session/token controls, and credential vaulting.	Approve identity policy, role assignments, exceptions, and ownership of human/non-human accounts.	User and privileged account inventory; MFA configuration; authentication policy; service-account records; password/authenticator settings; provisioning/deprovisioning tickets.
3.6 Incident Response (IR)	3	Establish an operational incident-handling capability, track/document/report incidents, and test incident	Operate SOC/service-desk detection, triage, containment, evidence preservation, technical recovery,	Own organizational incident plan, reporting decisions, management escalation, external communications, and acceptance of	Incident plan; tickets; timelines; evidence indexes; reporting procedures; tabletop results; lessons learned; corrective

		response.	incident tickets, and exercises within authorized scope.	recovery/closure.	actions; interviews and demonstrations.
3.7 Maintenance (MA)	6	Perform and control system maintenance, including maintenance tools, personnel, remote maintenance, and sanitization of equipment before offsite maintenance where required.	Manage authorized maintenance tools, technician access, remote sessions, maintenance records, and secure support procedures.	Define authorized maintenance and approval process; ensure customer equipment and CUI are protected during service.	Maintenance tickets; remote support logs; tool inventory; technician authorization; session records; sanitization procedures; vendor maintenance approvals.
3.8 Media Protection (MP)	9	Protect CUI on system media, control access, mark media as required, sanitize or destroy media, and control removable media and transport.	Implement removable-media controls, encryption, endpoint policies, media inventory support, secure wipe processes, and technical enforcement.	Define permitted media use, marking/handling rules, transport approval, disposition decisions, and organizational custody.	USB/device-control settings; encryption; media records; destruction/sanitization certificates; transport procedures; access restrictions; disposal tickets.
3.9 Personnel Security (PS)	2	Screen individuals before authorizing access and protect systems during and after personnel actions such as termination or transfer.	Execute technical onboarding/offboarding, account disablement, privilege removal, token/session revocation, device recovery, and access verification.	Perform personnel screening and HR decisions; notify technical teams promptly; authorize role changes and termination actions.	Onboarding/ offboarding records; termination tickets; access-removal evidence; screening policy/records as appropriate; role-change approvals.
3.10 Physical Protection (PE)	6	Limit physical access to systems, equipment, and operating environments; escort visitors; maintain access records; control physical access devices.	Support data-center/rack access where MSP facilities are in scope, maintain facility access systems, and coordinate secure equipment handling.	Own customer-site physical security, visitor processes, facility authorization, and physical boundaries unless specifically outsourced.	Badge/access records; visitor logs; facility diagrams; camera/access procedures; physical key/badge inventories; interviews and observation.
3.11 Risk Assessment (RA)	3	Periodically assess risk and scan for vulnerabilities; remediate vulnerabilities according to risk.	Operate vulnerability scanning, asset discovery, risk dashboards, remediation tickets, rescans, and technical prioritization.	Own organizational risk assessment, risk acceptance, business prioritization, and approval of exceptions.	Risk assessments; vulnerability scans; asset scope; remediation tickets; risk exceptions; rescan evidence; management review.
3.12 Security Assessment (CA)	4	Assess security controls, develop	Provide technical assessment	Own SSP, assessment results,	SSP; assessment results;

		and implement remediation plans, monitor controls, and maintain a system security plan.	evidence, remediation support, continuous-monitoring data, configuration evidence, and provider service descriptions.	organizational remediation decisions, POA&M governance, and overall system description.	POA&M/remediation records; continuous-monitoring reports; evidence index; architecture/data-flow diagrams; responsibility matrix.
3.13 System and Communications Protection (SC)	16	Protect communications at system boundaries and within systems, employ cryptography, separate functions, control connections, and protect CUI in transit.	Configure firewalls, segmentation, VPN, secure protocols, encryption, DNS/email/network security, boundary protection, and cloud security controls.	Define approved architecture, external connections, CUI flows, cryptographic requirements, and business exceptions.	Network diagrams; firewall/VPN configuration; encryption settings; approved connection inventory; segmentation tests; secure protocol settings; certificates.
3.14 System and Information Integrity (SI)	7	Identify, report, and correct flaws; protect against malicious code; monitor alerts; update protections; scan systems/files and detect unauthorized use.	Patch management, EDR/antimalware, vulnerability response, threat intelligence, monitoring, alert triage, and security-tool health.	Approve remediation priorities/exceptions, ensure assets are covered, and maintain organizational response to security advisories.	Patch reports; EDR status; malware alerts; vulnerability tickets; threat advisories; update settings; monitoring records; exception approvals.

K.10 Understanding the 110-Requirement Structure

The current CMMC Level 2 requirement set contains 110 NIST SP 800-171 Revision 2 security requirements distributed across fourteen families. The number of requirements in a family does not indicate its importance. A three-requirement family such as Incident Response can require substantial operational maturity, while a larger family such as Access Control contains many distinct access-management conditions.

Family	**Count**
3.1 Access Control	22
3.2 Awareness and Training	3
3.3 Audit and Accountability	9
3.4 Configuration Management	9
3.5 Identification and Authentication	11
3.6 Incident Response	3
3.7 Maintenance	6

3.8 Media Protection	9
3.9 Personnel Security	2
3.10 Physical Protection	6
3.11 Risk Assessment	3
3.12 Security Assessment	4
3.13 System and Communications Protection	16
3.14 System and Information Integrity	7
TOTAL	110

K.11 3.1 Access Control (AC)

This family contains 22 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to limit system access to authorized users, processes acting on behalf of authorized users, and authorized devices; control functions, remote access, wireless access, mobile devices, and CUI flow.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Identity platforms, directory services, MFA, VPN, conditional access, firewall rules, endpoint/device controls, RMM permissions, access reviews, and ticketed provisioning.

Typical Contractor / OSA Responsibility

Approved user/access policy, authorization decisions, business-role definitions, CUI flow decisions, exceptions, and periodic management review.

Representative Assessment Evidence

Account exports; group memberships; MFA/conditional-access configuration; VPN and firewall settings; access requests; termination tickets; privileged-access reviews; demonstrations of allowed and denied access.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.12 3.2 Awareness and Training (AT)

This family contains 3 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to ensure managers, administrators, users, and security personnel understand security risks, responsibilities, and role-specific duties.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Provide technical-security training for MSP technicians, document platform procedures, support phishing/security awareness platforms, and maintain technician competency records.

Typical Contractor / OSA Responsibility

Define required training, ensure personnel complete it, provide role-specific awareness, and retain organizational training evidence.

Representative Assessment Evidence

Training assignments and completion; role-based technician training; awareness communications; interview responses; exercise records.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.13 3.3 Audit and Accountability (AU)

This family contains 9 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to create, protect, review, and retain audit records needed to monitor, investigate, and report inappropriate or unauthorized activity.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Configure logging, centralize events, synchronize time, operate SIEM/SOC, protect logs, investigate alerts, and support retention.

Typical Contractor / OSA Responsibility

Determine audit needs and retention consistent with risk and requirements; ensure relevant systems are included; review provider service boundaries.

Representative Assessment Evidence

Logging configurations; SIEM source inventory; sample logs; alert tickets; time synchronization; retention settings; privileged audit access; review records.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.14 3.4 Configuration Management (CM)

This family contains 9 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to establish and maintain system baselines, control changes, restrict unnecessary functionality, and manage software and configuration settings.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Build secure baselines, deploy configuration policies, manage patches/configurations, maintain RMM/MDM policies, document changes, and detect drift.

Typical Contractor / OSA Responsibility

Approve baselines and business exceptions, define change authority, maintain system descriptions, and accept operational risk.

Representative Assessment Evidence

Baseline documents; configuration exports; change tickets; software inventory; prohibited software controls; exception approvals; before/after configuration evidence.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.15 3.5 Identification and Authentication (IA)

This family contains 11 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to identify users, devices, and processes and authenticate identities before access, including multifactor authentication and password/authenticator protections.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Operate directory/identity platforms, MFA, privileged identity, service-account controls, certificate/device identity, session/token controls, and credential vaulting.

Typical Contractor / OSA Responsibility

Approve identity policy, role assignments, exceptions, and ownership of human/non-human accounts.

Representative Assessment Evidence

User and privileged account inventory; MFA configuration; authentication policy; service-account records; password/authenticator settings; provisioning/deprovisioning tickets.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.16 3.6 Incident Response (IR)

This family contains 3 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to establish an operational incident-handling capability, track/document/report incidents, and test incident response.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Operate SOC/service-desk detection, triage, containment, evidence preservation, technical recovery, incident tickets, and exercises within authorized scope.

Typical Contractor / OSA Responsibility

Own organizational incident plan, reporting decisions, management escalation, external communications, and acceptance of recovery/closure.

Representative Assessment Evidence

Incident plan; tickets; timelines; evidence indexes; reporting procedures; tabletop results; lessons learned; corrective actions; interviews and demonstrations.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.17 3.7 Maintenance (MA)

This family contains 6 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to perform and control system maintenance, including maintenance tools, personnel, remote maintenance, and sanitization of equipment before offsite maintenance where required.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Manage authorized maintenance tools, technician access, remote sessions, maintenance records, and secure support procedures.

Typical Contractor / OSA Responsibility

Define authorized maintenance and approval process; ensure customer equipment and CUI are protected during service.

Representative Assessment Evidence

Maintenance tickets; remote support logs; tool inventory; technician authorization; session records; sanitization procedures; vendor maintenance approvals.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.18 3.8 Media Protection (MP)

This family contains 9 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to protect CUI on system media, control access, mark media as required, sanitize or destroy media, and control removable media and transport.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Implement removable-media controls, encryption, endpoint policies, media inventory support, secure wipe processes, and technical enforcement.

Typical Contractor / OSA Responsibility

Define permitted media use, marking/handling rules, transport approval, disposition decisions, and organizational custody.

Representative Assessment Evidence

USB/device-control settings; encryption; media records; destruction/sanitization certificates; transport procedures; access restrictions; disposal tickets.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.19 3.9 Personnel Security (PS)

This family contains 2 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to screen individuals before authorizing access and protect systems during and after personnel actions such as termination or transfer.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Execute technical onboarding/offboarding, account disablement, privilege removal, token/session revocation, device recovery, and access verification.

Typical Contractor / OSA Responsibility

Perform personnel screening and HR decisions; notify technical teams promptly; authorize role changes and termination actions.

Representative Assessment Evidence

Onboarding/offboarding records; termination tickets; access-removal evidence; screening policy/records as appropriate; role-change approvals.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.20 3.10 Physical Protection (PE)

This family contains 6 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to limit physical access to systems, equipment, and operating environments; escort visitors; maintain access records; control physical access devices.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Support data-center/rack access where MSP facilities are in scope, maintain facility access systems, and coordinate secure equipment handling.

Typical Contractor / OSA Responsibility

Own customer-site physical security, visitor processes, facility authorization, and physical boundaries unless specifically outsourced.

Representative Assessment Evidence

Badge/access records; visitor logs; facility diagrams; camera/access procedures; physical key/badge inventories; interviews and observation.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.21 3.11 Risk Assessment (RA)

This family contains 3 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to periodically assess risk and scan for vulnerabilities; remediate vulnerabilities according to risk.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Operate vulnerability scanning, asset discovery, risk dashboards, remediation tickets, rescans, and technical prioritization.

Typical Contractor / OSA Responsibility

Own organizational risk assessment, risk acceptance, business prioritization, and approval of exceptions.

Representative Assessment Evidence

Risk assessments; vulnerability scans; asset scope; remediation tickets; risk exceptions; rescan evidence; management review.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.22 3.12 Security Assessment (CA)

This family contains 4 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to assess security controls, develop and implement remediation plans, monitor controls, and maintain a system security plan.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Provide technical assessment evidence, remediation support, continuous-monitoring data, configuration evidence, and provider service descriptions.

Typical Contractor / OSA Responsibility

Own SSP, assessment results, organizational remediation decisions, POA&M governance, and overall system description.

Representative Assessment Evidence

SSP; assessment results; POA&M/remediation records; continuous-monitoring reports; evidence index; architecture/data-flow diagrams; responsibility matrix.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.23 3.13 System and Communications Protection (SC)

This family contains 16 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to protect communications at system boundaries and within systems, employ cryptography, separate functions, control connections, and protect CUI in transit.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Configure firewalls, segmentation, VPN, secure protocols, encryption, DNS/email/network security, boundary protection, and cloud security controls.

Typical Contractor / OSA Responsibility

Define approved architecture, external connections, CUI flows, cryptographic requirements, and business exceptions.

Representative Assessment Evidence

Network diagrams; firewall/VPN configuration; encryption settings; approved connection inventory; segmentation tests; secure protocol settings; certificates.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.24 3.14 System and Information Integrity (SI)

This family contains 7 NIST SP 800-171 Revision 2 security requirements. In practical terms, its core outcome is to identify, report, and correct flaws; protect against malicious code; monitor alerts; update protections; scan systems/files and detect unauthorized use.

For an MSP, the important question is not simply whether a product is installed. The implementation must connect policy and authorization to actual technical behavior, recurring operations, and evidence.

Typical MSP Operational Contribution

Patch management, EDR/antimalware, vulnerability response, threat intelligence, monitoring, alert triage, and security-tool health.

Typical Contractor / OSA Responsibility

Approve remediation priorities/exceptions, ensure assets are covered, and maintain organizational response to security advisories.

Representative Assessment Evidence

Patch reports; EDR status; malware alerts; vulnerability tickets; threat advisories; update settings; monitoring records; exception approvals.

Assessment Preparation Questions

- What systems, identities, services, and providers are actually in scope for this family?
- Which party decides the requirement's implementation and which party performs the recurring work?
- What document describes the implementation and does it match the real environment?
- What evidence demonstrates operation over time rather than only a point-in-time configuration?
- Which technician, administrator, manager, or user could explain the implementation during an interview?
- What could an assessor reasonably test, and would the observed behavior match the documented design?

K.25 Cross-Reference: Requirement → Implementation → Evidence → Assessment

Layer	Question to Ask	MSP Example
Requirement	What outcome must be achieved?	Restrict access, protect logs, patch flaws, or respond to incidents.
Assessment objective	What specific determination must the assessor make?	Determine whether required conditions are defined and implemented.
Implementation	What actually performs the requirement?	Identity policy, firewall rule, EDR configuration, ticket workflow, backup procedure.
Evidence	What proves it exists and operates?	Configuration export, ticket, log, approval, report, exercise, screenshot.
Interview	Who can explain it?	Technician, security engineer, customer system owner, manager.
Test	What behavior can be demonstrated?	MFA challenge, denied access, session lock, restored backup, generated alert.

K.26 Party ABC Example — Building a Cross-Reference Record

Party ABC uses Party IJK for identity, endpoint protection, vulnerability management, SIEM monitoring, backup, and incident-response support. ABC should not write “MSP handles CMMC” in its SSP. Instead, it should identify the applicable requirements and describe the actual implementation and responsibility boundary.

For an identity requirement, ABC may define who is authorized and approve roles. Party IJK may configure the identity platform, MFA, conditional access, and privileged groups. Evidence may include ABC's access approval, Party IJK's change ticket, identity configuration, account export, and a demonstration. The cross-reference becomes a map between the official requirement and real operations.

K.27 Party EGH Example — Why a Product Name Is Not a Cross-Reference

Party EGH states that it satisfies System and Information Integrity because it purchased EDR. That statement is incomplete. The relevant requirements include identifying and correcting flaws, malicious-code protection, monitoring security alerts, updating protection mechanisms, scanning, and identifying unauthorized use.

The cross-reference should therefore identify which EDR functions contribute to which requirements, what patch or vulnerability processes cover the remaining outcomes, who monitors alerts, what happens when a detection occurs, and what evidence shows those activities. Technology supports the requirement; it does not replace the requirement.

K.28 Party IJK Example — One MSP Service Supporting Multiple Families

A managed SIEM/SOC service may contribute to Audit and Accountability, Incident Response, and System and Information Integrity. That does not mean one dashboard proves all three families. Audit evidence may focus on log generation, protection, retention, review, and time synchronization. Incident-response evidence may focus on triage, escalation, documentation, and response. Integrity evidence may focus on monitoring security alerts and identifying unauthorized use.

This is why evidence should be indexed by requirement and assessment objective rather than stored as an undifferentiated folder of screenshots.

K.29 Cross-Reference Worksheet Template

Requirement ID	Requirement Outcome	Implementation	Owner/ Decision	Operator	Evidence	Examine	Interview	Test	Gap/ Action

3.x.x									
3.x.x									
3.x.x									

K.30 MSP Responsibility Mapping Template

Requirement/ Family	Customer Owns/Decides	MSP Implements	MSP Operates	Evidence Producer	Evidence Owner	Assessment Participant

K.31 Evidence Index Template

Requirement	Evidence ID	Artifact	Source System/Owner	Date/Period	Assessment Method	Location	Notes

K.32 Common Cross-Reference Mistakes

- Treating a product purchase as proof that a security requirement is satisfied.
- Mapping an entire family to one policy without technical or operational evidence.
- Assigning every requirement to the MSP without documenting customer decisions and accountability.
- Using screenshots that do not identify the system, date, scope, or configuration being demonstrated.
- Building the cross-reference immediately before assessment instead of maintaining it as operations change.
- Assuming NIST SP 800-171 Revision 3 has automatically replaced Revision 2 for the current CMMC Level 2 assessment basis.

- Listing evidence without connecting it to assessment objectives, interviews, and tests.
- Failing to update the SSP and responsibility matrix when cloud, MSP, SOC, backup, identity, or network architecture changes.

K.33 How to Maintain the Cross-Reference

The cross-reference should be treated as a living operational index. Changes to architecture, providers, security tools, responsibility assignments, CUI flows, or major procedures should trigger review of the affected mappings. Periodic readiness reviews can then verify that the evidence named in the cross-reference still exists and remains representative.

For Party IJK, maintaining customer-specific mappings also improves service delivery. The MSP can see which recurring tickets, reports, exports, and reviews produce useful evidence and can identify gaps before an assessment window.

K.34 Current Regulatory and Publication Caution

As verified September 22, 2026, current Department CMMC materials state that Phase II implementation was suspended July 13, 2026 and that Phase I self-assessment requirements remain in place. The Department currently states that Level 2 uses the 110 security requirements in NIST SP 800-171 Revision 2. NIST itself withdrew Revision 2 in May 2024 and superseded it with Revision 3. These facts are not contradictory: NIST publication lifecycle and the current CMMC contractual/program baseline are separate matters.

Because the CMMC program is under review, this appendix must be rechecked against current Department guidance, 32 CFR part 170, applicable DFARS clauses, the current CMMC Assessment Guide, and the specific solicitation or contract before final publication or operational use.

K.35 Authoritative Sources for This Teaching Edition

- NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations; NIST CSRC notes Revision 2 was withdrawn May 14, 2024 and superseded by Revision 3.
- CMMC Assessment Guide – Level 2, Version 2.13, Department CMMC program resources.

- Current CMMC About and Resources & Documentation pages, Department CMMC program, verified September 22, 2026.
- DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025), Acquisition.gov.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program.

K.36 Final Teaching Perspective

The most useful CMMC/NIST cross-reference is not a compliance spreadsheet filled with product names. It is a traceability model connecting each security requirement to the organization's real architecture, decisions, operating procedures, evidence, people, and assessment behavior.

For an MSP, this creates clarity. Party IJK can identify exactly where it contributes and exactly what evidence its services produce. Party ABC and Party EGH can see what remains an organizational responsibility. Assessors can follow the implementation from requirement to evidence without guessing. That is the purpose of this appendix and the standard the deeper version will continue to build upon.

K.37 Deepening Pass — Requirement-by-Requirement Traceability

This deepening pass extends the family-level model into a working index for all 110 NIST SP 800-171 Revision 2 requirements used by the current CMMC Level 2 program. The “Operational Focus” descriptions below are concise teaching paraphrases, not replacements for the normative NIST requirement text. Final assessment preparation should always use the official NIST publication and current CMMC Assessment Guide for the exact requirement and assessment objectives.

The table deliberately separates the requirement identifier from the MSP contribution and evidence. This prevents a common error in which a tool name is treated as the requirement itself. The MSP contribution describes work Party IJK might perform; the customer/OSA still needs to document the actual responsibility allocation for its environment.

K.37.1 Access Control — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.1.1	Authorized users, processes, and devices	Implement and operate assigned technical safeguards; maintain customer-specific records	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as	Examine / Interview / Test as selected by the current Assessment Guide

		and evidence.	applicable.	
3.1.2	Authorized transactions and functions	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.3	CUI information-flow enforcement	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.4	Separation of duties	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.5	Least privilege	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.6	Use nonprivileged accounts for nonsecurity functions	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.7	Prevent/audit privileged functions by nonprivileged users	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.8	Unsuccessful logon limits	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.9	Privacy/security notices	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.10	Session lock	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.11	Automatic session termination	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.12	Monitor/control remote access	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and	Account/group export; policy/configuration; approval ticket; MFA/access review;	Examine / Interview / Test as selected by the current Assessment Guide

		technical evidence.	demonstration.	
3.1.13	Cryptographic protection for remote access	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.14	Managed remote-access points	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.15	Authorize remote privileged commands/security information	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.16	Authorize wireless access	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.17	Protect wireless with authentication/encryption	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.18	Control mobile-device connections	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.19	Encrypt CUI on mobile devices	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.20	Control external-system connections/use	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.21	Limit portable storage on external systems	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.1.22	Control CUI on publicly accessible systems	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.2 Awareness and Training — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.2.1	Security awareness	Technician role training and support for customer awareness platforms; retain completion evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.2.2	Role-based security training	Technician role training and support for customer awareness platforms; retain completion evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.2.3	Insider-threat awareness	Technician role training and support for customer awareness platforms; retain completion evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.3 Audit and Accountability — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.3.1	Create/retain audit records	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.3.2	Unique traceability to users	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.3.3	Review/update logged events	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.3.4	Alert on audit-process failure	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.3.5	Correlate audit review/investigation/reporting	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide

3.3.6	Audit reduction/reporting	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.3.7	Authoritative time source/time stamps	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.3.8	Protect audit information/tools	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.3.9	Limit audit-management functionality	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.4 Configuration Management — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.4.1	Baseline configurations/inventories	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.4.2	Security configuration settings	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.4.3	Track/review/approve/log changes	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.4.4	Analyze security impact before change	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.4.5	Define/enforce change-access restrictions	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.4.6	Least functionality	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and	Baseline; configuration export; change ticket; inventory; exception/approval; drift	Examine / Interview / Test as selected by the current Assessment Guide

		tickets.	report.	
3.4.7	Restrict/disable unnecessary functions/services/ports	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.4.8	Software allow/deny controls	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.4.9	Control user-installed software	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.5 Identification and Authentication — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.5.1	Identify users/devices/processes	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.2	Authenticate identities	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.3	Multifactor authentication	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.4	Replay-resistant authentication	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.5	Prevent identifier reuse	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.6	Disable identifiers after inactivity	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.7	Password complexity	Identity/IAM configuration, access tickets, MFA,	Account/group export; policy/configuration;	Examine / Interview / Test as selected by the current

		privileged-access operations, reviews, and technical evidence.	approval ticket; MFA/access review; demonstration.	Assessment Guide
3.5.8	Prevent password reuse	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.9	Temporary passwords changed immediately	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.10	Cryptographically protected passwords	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.5.11	Obscure authentication feedback	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.6 Incident Response — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.6.1	Operational incident-handling capability	SOC triage, escalation, authorized containment, evidence preservation, technical recovery, and incident records.	IR plan; incident ticket/timeline; evidence index; exercise; lessons learned; reporting procedure.	Examine / Interview / Test as selected by the current Assessment Guide
3.6.2	Track/document/report incidents	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.6.3	Test incident-response capability	SOC triage, escalation, authorized containment, evidence preservation, technical recovery, and incident records.	IR plan; incident ticket/timeline; evidence index; exercise; lessons learned; reporting procedure.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.7 Maintenance — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.7.1	Perform system maintenance	Authorized maintenance tooling, remote support controls, technician records, and maintenance tickets.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as	Examine / Interview / Test as selected by the current Assessment Guide

			applicable.	
3.7.2	Control maintenance tools/personnel	Authorized maintenance tooling, remote support controls, technician records, and maintenance tickets.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.7.3	Sanitize equipment for offsite maintenance	Authorized maintenance tooling, remote support controls, technician records, and maintenance tickets.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.7.4	Check diagnostic/test media for malicious code	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Scan/EDR report; patch record; remediation ticket; rescan; exception approval.	Examine / Interview / Test as selected by the current Assessment Guide
3.7.5	Require MFA for nonlocal maintenance; terminate sessions	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.7.6	Supervise unauthorized maintenance personnel	Authorized maintenance tooling, remote support controls, technician records, and maintenance tickets.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.8 Media Protection — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.8.1	Protect system media	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Encryption/device-control settings; media/backup record; custody or sanitization evidence.	Examine / Interview / Test as selected by the current Assessment Guide
3.8.2	Limit media access	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.8.3	Sanitize/destroy media before disposal/reuse	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Encryption/device-control settings; media/backup record; custody or sanitization evidence.	Examine / Interview / Test as selected by the current Assessment Guide
3.8.4	Mark media with CUI markings/distribution limits	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Encryption/device-control settings; media/backup record; custody or sanitization evidence.	Examine / Interview / Test as selected by the current Assessment Guide
3.8.5	Control media access during transport	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide

3.8.6	Cryptographically protect CUI on digital media during transport	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.8.7	Control removable media	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Encryption/device-control settings; media/backup record; custody or sanitization evidence.	Examine / Interview / Test as selected by the current Assessment Guide
3.8.8	Prohibit unidentifiable portable storage	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.8.9	Protect backup CUI confidentiality	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Encryption/device-control settings; media/backup record; custody or sanitization evidence.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.9 Personnel Security — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.9.1	Screen individuals before system access	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.9.2	Protect systems during/after personnel actions	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.10 Physical Protection — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.10.1	Limit physical access	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.10.2	Protect/monitor facility and support infrastructure	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.10.3	Escort/monitor visitors	Logging/SIEM configuration, source health, alert operations, retention support, tickets,	Log-source inventory; sample records; SIEM config; alert/ticket;	Examine / Interview / Test as selected by the current Assessment Guide

		and exported evidence.	retention/time settings.	
3.10.4	Maintain physical-access logs	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.10.5	Control/manage physical-access devices	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.10.6	Safeguard CUI at alternate work sites	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.11 Risk Assessment — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.11.1	Periodic risk assessment	Technical evidence, monitoring reports, remediation support, architecture/service descriptions, and gap tracking.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.11.2	Vulnerability scanning	Scanning, patching, EDR/antimalware, remediation tickets, rescans, and exception tracking.	Scan/EDR report; patch record; remediation ticket; rescan; exception approval.	Examine / Interview / Test as selected by the current Assessment Guide
3.11.3	Remediate vulnerabilities according to risk	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Scan/EDR report; patch record; remediation ticket; rescan; exception approval.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.12 Security Assessment — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.12.1	Assess security controls	Technical evidence, monitoring reports, remediation support, architecture/service descriptions, and gap tracking.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.12.2	Develop/implement remediation plans	Encryption/device control, backup operations, media handling support, secure wipe, and custody evidence.	Encryption/device-control settings; media/backup record; custody or sanitization evidence.	Examine / Interview / Test as selected by the current Assessment Guide
3.12.3	Monitor security controls	Logging/SIEM	Log-source inventory;	Examine / Interview / Test

		configuration, source health, alert operations, retention support, tickets, and exported evidence.	sample records; SIEM config; alert/ticket; retention/time settings.	as selected by the current Assessment Guide
3.12.4	Develop/update system security plan	Technical evidence, monitoring reports, remediation support, architecture/service descriptions, and gap tracking.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.13 System and Communications Protection — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.13.1	Monitor/control/protect communications at boundaries	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.2	Architectural/security engineering principles	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.3	Separate user and system-management functionality	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.4	Prevent unauthorized/unintended information transfer via shared resources	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.5	Separate public system components from internal networks	Firewall/VPN/network security, encryption, key/certificate operations, segmentation, and configuration evidence.	Diagram; firewall/VPN config; encryption/certificate setting; connection inventory; test.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.6	Deny network traffic by default/allow by exception	Firewall/VPN/network security, encryption, key/certificate operations, segmentation, and configuration evidence.	Diagram; firewall/VPN config; encryption/certificate setting; connection inventory; test.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.7	Prevent split tunneling for remote devices	Firewall/VPN/network security, encryption, key/certificate operations, segmentation, and configuration evidence.	Diagram; firewall/VPN config; encryption/certificate setting; connection inventory; test.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.8	Protect CUI in transit with cryptography	Firewall/VPN/network security, encryption, key/certificate operations, segmentation, and	Diagram; firewall/VPN config; encryption/certificate setting; connection	Examine / Interview / Test as selected by the current Assessment Guide

		configuration evidence.	inventory; test.	
3.13.9	Terminate network connections at session end/inactivity	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.10	Establish/manage cryptographic keys	Firewall/VPN/network security, encryption, key/certificate operations, segmentation, and configuration evidence.	Diagram; firewall/VPN config; encryption/certificate setting; connection inventory; test.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.11	Use FIPS-validated cryptography when protecting CUI confidentiality	Firewall/VPN/network security, encryption, key/certificate operations, segmentation, and configuration evidence.	Diagram; firewall/VPN config; encryption/certificate setting; connection inventory; test.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.12	Prohibit remote activation of collaborative-device indicators; provide use indication	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.13	Control mobile code	Firewall/VPN/network security, encryption, key/certificate operations, segmentation, and configuration evidence.	Diagram; firewall/VPN config; encryption/certificate setting; connection inventory; test.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.14	Control VoIP technologies	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.15	Protect authenticity of communications sessions	Identity/IAM configuration, access tickets, MFA, privileged-access operations, reviews, and technical evidence.	Account/group export; policy/configuration; approval ticket; MFA/access review; demonstration.	Examine / Interview / Test as selected by the current Assessment Guide
3.13.16	Protect confidentiality of CUI at rest	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide

K.37.14 System and Information Integrity — Detailed Requirement Index

ID	Operational Focus (Paraphrase)	Typical Party IJK Contribution	Representative Evidence	Assessment Lens
3.14.1	Identify/report/correct system flaws	Baseline/RMM/MDM configuration, change control, software inventory, hardening, drift review, and tickets.	Baseline; configuration export; change ticket; inventory; exception/approval; drift report.	Examine / Interview / Test as selected by the current Assessment Guide
3.14.2	Malicious-code protection	Scanning, patching, EDR/antimalware,	Scan/EDR report; patch record; remediation ticket;	Examine / Interview / Test as selected by the current

		remediation tickets, rescans, and exception tracking.	rescan; exception approval.	Assessment Guide
3.14.3	Monitor security alerts/advisories and act	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.14.4	Update malicious-code protection	Scanning, patching, EDR/antimalware, remediation tickets, rescans, and exception tracking.	Scan/EDR report; patch record; remediation ticket; rescan; exception approval.	Examine / Interview / Test as selected by the current Assessment Guide
3.14.5	Periodic/real-time scans	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.14.6	Monitor systems/communications for attacks and indicators	Logging/SIEM configuration, source health, alert operations, retention support, tickets, and exported evidence.	Log-source inventory; sample records; SIEM config; alert/ticket; retention/time settings.	Examine / Interview / Test as selected by the current Assessment Guide
3.14.7	Identify unauthorized system use	Implement and operate assigned technical safeguards; maintain customer-specific records and evidence.	Policy/procedure; configuration or operational record; ticket/report; interview; demonstration as applicable.	Examine / Interview / Test as selected by the current Assessment Guide

K.38 Deepening Pass — How to Use the 110-Requirement Index

Start with the official requirement and its assessment objectives. Then identify the in-scope assets and services that implement it. Next assign who decides, implements, operates, produces evidence, maintains evidence, and participates in assessment. Finally, link specific evidence to the objective it supports. If one artifact supports several requirements, index it separately under each relevant requirement rather than assuming one appearance proves all of them.

For Party ABC, this can turn a large CMMC readiness project into a controlled traceability exercise. For Party IJK, it turns recurring managed-service work into predictable evidence production. The same access review, vulnerability remediation ticket, SIEM investigation, backup test, or change record can become high-quality assessment evidence when it is complete, dated, attributable, and connected to the correct requirement.

K.39 Deepening Pass — Evidence Sufficiency Test

Question	Strong Answer Looks Like

Is the artifact relevant?	It directly supports a specific requirement or assessment objective.
Is it attributable?	The system, customer, actor, source, and/or owner can be identified.
Is it current enough?	It represents the assessed environment and appropriate operating period.
Is it complete?	Important context is not missing from a cropped screenshot or isolated export.
Does it show operation?	Recurring records demonstrate that the process works over time.
Can personnel explain it?	Interviewed staff understand the implementation and responsibility boundary.
Can behavior be demonstrated?	Where testing is selected, the mechanism behaves as documented.

K.40 Deepening Pass — Requirement Ownership Is Not Binary

A single requirement can contain several responsibility layers. Party ABC may define authorized users, Party IJK may provision the accounts, a cloud identity provider may enforce authentication, Party IJK's SOC may monitor identity events, and ABC management may review exceptions. Calling the requirement simply “MSP-owned” hides these distinctions.

The responsibility model used throughout this book—who owns, decides, implements, operates, produces evidence, maintains evidence, and independently assesses—should therefore be applied at the requirement or assessment-objective level when the implementation is complex.

K.41 Deepening Pass — Cross-Family Dependencies

Requirements do not operate in isolation. Access Control depends on Identification and Authentication. Audit and Accountability supports Incident Response and System and Information Integrity. Configuration Management affects vulnerability remediation and boundary protection. Personnel Security triggers identity and access changes. Security Assessment depends on evidence generated across every technical family.

The cross-reference should capture these dependencies without double-counting evidence. For example, a SIEM alert may demonstrate monitoring under System and Information Integrity while the underlying audit-source configuration supports Audit and Accountability. The incident ticket created from that alert may then support Incident Response.

K.42 Deepening Pass — Party ABC Traceability Example

Assume Party ABC authorizes remote administrative support only for designated Party IJK technicians. ABC's governance record identifies the authorized service and roles. Party IJK configures its RMM platform and identity groups so only those technicians can initiate the approved remote functions, requires MFA, records sessions, and periodically reviews privileged membership.

The cross-reference would not point to “RMM” as the answer. It would identify the applicable access, authentication, audit, maintenance, and communications-protection requirements; map each implementation element; and link the relevant approvals, configuration exports, logs, tickets, and demonstrations. This creates a defensible chain from requirement to operation.

K.43 Deepening Pass — Party EGH Gap Example

Party EGH has MFA for employees but discovers that two legacy service accounts and one emergency administrator use different authentication paths. A family-level statement saying “MFA enabled” can conceal this gap. The requirement-level index forces EGH and Party IJK to identify which identities are covered, which are exceptions, what compensating architecture exists, and whether the current implementation satisfies the exact assessment objectives.

The correct outcome is not to manufacture a screenshot. It is to understand the gap, remediate it where required, and preserve the resulting implementation evidence.

K.44 Deepening Pass — Assessment Interview Preparation

The requirement index can also be used to identify the best interviewee. The person who wrote the policy may not be the person who can explain firewall administration, account provisioning, EDR operations, or backup restoration. Each requirement should identify personnel who actually understand the implementation.

Interview preparation should teach personnel to explain normal work accurately, not memorize scripted answers. A technician should be able to describe what triggers an account change, how authorization is verified, what system enforces it, what evidence is produced, and how exceptions are escalated.

K.45 Deepening Pass — Assessment Test Preparation

For requirements likely to involve testing, the team should know what safe demonstration can be performed without disrupting production. Examples include demonstrating MFA, showing that unauthorized access is denied, verifying session lock behavior, generating a test alert, demonstrating a controlled restore, or showing that an approved configuration is enforced.

A demonstration environment should faithfully represent the assessed implementation. Staging a special configuration solely for assessment that differs from production undermines the purpose of testing.

K.46 Deepening Pass — Maintaining the Index Through Change

The 110-requirement cross-reference should be reviewed when Party ABC changes identity providers, migrates to a new cloud environment, changes MSPs, adds a SOC, modifies network boundaries, replaces endpoint security, introduces new CUI workflows, or changes responsibility assignments. Those events can affect many requirements at once.

Party IJK can incorporate cross-reference maintenance into change management. A significant service change should identify which customer requirements, SSP sections, diagrams, evidence sources, and assessment demonstrations may need revision.

K.47 Deepening Pass — Verification Note

This edition contains 110 requirement-level entries, matching the current Department CMMC Level 2 statement that the program uses 110 NIST SP 800-171 Revision 2 security requirements. NIST identifies Revision 2 as withdrawn and superseded by Revision 3, while current Department CMMC materials continue to use Revision 2 for the Level 2 baseline. The exact normative requirement language and assessment objectives remain in the official publications and are intentionally not reproduced wholesale here.

K.48 Substantive Pass — Turning the Cross-Reference into an MSP Operating Model

The requirement index becomes most valuable when it is connected to the MSP's recurring service catalog. Party IJK should be able to identify which managed

services contribute to which requirements, what customer decisions those services depend upon, what recurring activities keep the implementation effective, and what evidence is produced naturally during operation.

For example, managed identity service can contribute to Access Control and Identification and Authentication, but the service must be decomposed into provisioning, privileged access, MFA, session controls, service accounts, access reviews, termination, and exception handling. Each activity produces different evidence and may involve different customer approvals.

Managed Service	Primary Families	Recurring Operational Activities	Representative Evidence
Identity/IAM	AC, IA, PS	Provision/deprovision, MFA, privileged groups, service accounts, access reviews	Approved request, account export, MFA configuration, review record, termination ticket
RMM/Endpoint Management	AC, CM, MA, SI	Baseline enforcement, software control, remote support, patching, health monitoring	RMM policy, inventory, change ticket, patch report, remote-session record
EDR/MDR	IR, SI, AU	Malware protection, detection, investigation, containment, alert monitoring	EDR health, alert record, investigation ticket, containment action, exception
SIEM/SOC	AU, IR, SI	Log collection, correlation, monitoring, escalation, investigation	Source inventory, retention setting, alert ticket, investigation chronology, log sample
Vulnerability Management	RA, SI, CM	Scanning, prioritization, remediation tracking, rescanning	Scan report, asset scope, remediation ticket, exception, rescan
Backup/Recovery	MP, IR, SC	Backup protection, recovery testing, incident recovery, encryption	Backup status, restore test, encryption configuration, recovery ticket
Network Security	AC, SC, AU	Firewalling, segmentation, VPN, boundary protection, logging	Diagram, firewall/VPN configuration, rule review, connection inventory, log evidence
Cloud Administration	AC, IA, AU, CM, SC, SI	Tenant configuration, identity, logging, sharing, encryption, app/service-principal control	Tenant config, role export, audit settings, sharing policy, change record
Incident Response	IR, AU, SI	Triage, evidence preservation, containment, recovery, lessons learned	Incident plan, ticket, timeline, evidence index, after-action report

K.49 Substantive Pass — Customer/MSP Responsibility Decomposition

Responsibility should be decomposed into decision, implementation, operation, evidence production, evidence custody, and assessment participation. This avoids the misleading statement that a requirement is simply “owned by the MSP.”

Responsibility Layer	Party ABC / EGH Example	Party IJK Example
Own/account for requirement	Maintain organizational implementation and SSP representation	Support only within contracted service boundary
Decide	Approve users, architecture, exceptions, risk decisions	Recommend technical implementation and escalation
Implement	Approve organizational policy and business workflow	Configure assigned platforms and safeguards
Operate	Perform customer governance/reviews	Run monitoring, patching, IAM, backup, or other assigned service
Produce evidence	Approvals, policy, management review	Tickets, logs, exports, reports, configuration records
Maintain evidence	Organizational evidence repository	Provider operational systems and customer-specific exports
Assessment participation	System owner, management, users	Technicians/engineers explain assigned implementation

K.50 Substantive Pass — Evidence Packages by Family

Family	Suggested Assessment Evidence Package
Access Control	Access policy; authorized-user list; privileged groups; access approvals; remote-access configuration; access-review records; termination evidence; sample allowed/denied demonstration.
Awareness and Training	Training policy; assigned curricula; completion reports; role-based administrator training; awareness communications; interview-ready explanation of responsibilities.
Audit and Accountability	Log-source inventory; event-selection rationale; sample audit records; SIEM configuration; retention; time synchronization; alert/review records; privileged audit access.
Configuration Management	Approved baselines; inventories; hardening settings; change tickets; security-impact review; software controls; exceptions; drift/remediation records.
Identification and Authentication	Identity inventory; MFA; authenticator policy; service-account records; password/authentication settings; provisioning and deprovisioning evidence.
Incident Response	IR plan; contacts; incident records; timelines; escalation; reporting procedure; exercises; lessons learned; corrective actions.
Maintenance	Maintenance policy; authorized tools; remote-maintenance controls; technician authorization; maintenance tickets; media checks and sanitization where applicable.
Media Protection	Media policy; removable-media controls; encryption; media inventory; transport/custody records; sanitization/destruction; backup confidentiality.
Personnel Security	Screening process evidence as appropriate; onboarding/role-change/termination notifications; access-removal tickets and verification.
Physical Protection	Facility boundary; authorized access; visitor process; access logs; physical access devices; alternate-work-site protections.

Risk Assessment	Risk assessment; vulnerability scope; scan reports; prioritization; remediation tickets; exceptions; rescans and management review.
Security Assessment	SSP; assessment results; remediation plan/POA&M where applicable; continuous-monitoring records; diagrams; provider responsibility documentation.
System and Communications Protection	Network/data-flow diagrams; boundary rules; VPN; segmentation; encryption; key/certificate settings; approved connections; secure protocol evidence.
System and Information Integrity	Patch/flaw remediation; EDR/antimalware health; advisories; monitoring; scans; detection/investigation records; unauthorized-use response.

K.51 Substantive Pass — Likely Interviewees by Family

Family	**Likely Customer Interviewees**	**Likely MSP Interviewees**
AC / IA	System owner, security lead, HR/request approver, selected users	IAM administrator, service desk lead, privileged-access engineer
AU / SI	Security lead, system owner	SOC analyst, SIEM engineer, endpoint security engineer
CM / RA	Change authority, system owner, risk owner	RMM/MDM engineer, vulnerability analyst, patch engineer
IR	Incident coordinator, management decision-maker	SOC/incident lead, service desk, forensic/security engineer
MA	System owner	Field/remote support technician, service manager
MP	Information owner, records/security personnel	Endpoint/device-control or backup administrator
PS	HR/security management	Onboarding/offboarding technical lead
PE	Facility/security personnel	Provider facility/security personnel if provider location is in scope
CA	SSP/system owner, compliance lead, management	Technical service owners supplying evidence
SC	Network/system owner	Network/cloud/security engineer
AT	Training owner, users, administrators	MSP technician/service manager for provider training

K.52 Substantive Pass — Safe Assessment Demonstrations

A test demonstration should prove normal implementation without creating unnecessary production risk. The team should agree in advance which demonstrations are safe, which require a maintenance window, and which can be shown in a representative but faithful environment.

- Demonstrate MFA for a normal or administrative login without exposing credentials.
- Show that a non-authorized account cannot perform a privileged function.
- Demonstrate session lock or timeout behavior where applicable.
- Show a controlled access provisioning and removal workflow from authorization through technical completion.
- Generate or identify a safe test security event and show its arrival in the monitoring workflow.
- Demonstrate a controlled restore from backup and the validation record.
- Show enforcement of a baseline or software restriction without changing production unnecessarily.
- Demonstrate remote-support authorization, authentication, logging, and termination.
- Show a vulnerability moving from detection through remediation and rescan.

K.53 Substantive Pass — Evidence Freshness and Operating Period

Point-in-time configuration evidence can show that a setting exists, but many requirements also depend on recurring operation. A strong package therefore combines configuration with records across the relevant operating period. Access reviews, vulnerability remediation, incident tickets, backup tests, monitoring investigations, change approvals, and training completion demonstrate that the implementation is lived rather than staged.

The cross-reference should identify whether an artifact is static design evidence, current configuration evidence, or recurring operational evidence. That distinction helps Party ABC avoid submitting twenty screenshots of settings while having no evidence that the associated process operates.

K.54 Substantive Pass — Evidence Quality Scoring Without Turning It into a Compliance Score

An internal readiness team can classify evidence quality without assigning a prohibited or misleading “CMMC score.” A practical evidence-quality status can be descriptive: missing, identified but not collected, collected but incomplete, current and attributable, or validated through interview/test. The purpose is workflow management, not a substitute for the official assessment methodology.

Evidence Status	Meaning	Next Action

Missing	No artifact has been identified	Determine implementation and evidence source
Identified	Source is known but artifact not collected/indexed	Collect and index
Incomplete	Artifact exists but lacks context, attribution, period, or objective coverage	Supplement or replace
Current / Attributable	Artifact clearly represents current scoped implementation	Validate against objective
Validated	Evidence aligns with documentation and can be explained/demonstrated	Maintain through assessment

K.55 Substantive Pass — Cross-Reference Change Triggers

- New MSP, MSSP, SOC, CSP, backup provider, or other external service provider.
- Migration between commercial cloud, GCC, GCC High, or another hosting environment.
- New identity provider, MFA method, privileged-access platform, or federation model.
- Replacement of EDR, SIEM, vulnerability scanner, RMM, firewall, VPN, or backup platform.
- New CUI workflow, application, business unit, facility, enclave, or external connection.
- Material network segmentation or boundary change.
- Change in responsibility between customer and provider.
- Major incident or assessment finding that changes the implementation.
- Onboarding or offboarding of a provider that holds evidence or operates security capabilities.

K.56 Substantive Pass — Party ABC End-to-End Requirement Traceability

Party ABC uses Party IJK to administer Microsoft identity, endpoint management, EDR, SIEM, vulnerability management, backup, and network security. ABC begins with an official requirement and its assessment objectives. It identifies the systems and services involved, then records ABC's policy and authorization role and Party IJK's implementation and operational role.

For a privileged-access requirement, ABC's management approves which job roles may receive privileged access. Party IJK provisions a named administrator through the approved IAM process, enforces MFA, limits membership to the appropriate

group, and records the change. SIEM monitoring records privileged authentication and selected administrative activity. Periodic review verifies that the membership remains appropriate.

The evidence package therefore includes the governing access rule, authorization, technical group export, MFA configuration, provisioning ticket, monitoring evidence, periodic review, and an interview/test path. No single screenshot is treated as the entire implementation.

K.57 Substantive Pass — Party EGH Remediation Traceability

Party EGH's vulnerability scan identifies an unsupported application on a CUI workstation. The cross-reference connects the finding to configuration management, risk assessment, and system/information integrity activities. Party IJK creates a remediation ticket, identifies the application owner, evaluates the required replacement or upgrade, and records the change.

If EGH temporarily cannot remove the application because of a production dependency, EGH—not Party IJK acting alone—makes the appropriate organizational risk/remediation decision under the applicable process. Party IJK documents technical compensating measures and continues tracking. Once the application is removed or upgraded, a rescan and configuration inventory provide closure evidence.

K.58 Substantive Pass — Party IJK Evidence Factory

An MSP should design recurring service processes so that useful evidence is a by-product of good operations. A well-structured access ticket records requestor, approver, account, role, technician, date, action, and verification. A vulnerability ticket records finding, affected asset, severity, decision, remediation, and rescan. A backup test records system, recovery point, method, result, validation, and corrective action.

This approach is more sustainable than asking technicians to create special compliance screenshots months later. The MSP's PSA, RMM, SIEM, IAM, EDR, vulnerability, and backup systems become controlled evidence sources, provided the records are complete and customer-specific.

K.59 Substantive Pass — Cross-Reference Review Meeting

A quarterly or pre-assessment cross-reference review can be organized by family or service. The team reviews changed architecture, open gaps, evidence freshness, responsibility changes, interview coverage, test readiness, and unresolved exceptions. The meeting should result in assigned actions rather than a general statement that the organization is “ready.”

For Party IJK, the review should include customer-specific service owners. The IAM engineer may validate AC/IA evidence, the SOC lead AU/IR/SI evidence, the network engineer SC evidence, and the service manager onboarding/offboarding and responsibility records.

K.60 Substantive Pass — Master Implementation and Evidence Record Template

Requirement ID	Official Objective Reference	Scoped Assets/Services	Customer Decision/Owner	MSP Implementation	Recurring Operation	Evidence IDs	Interviewee	Safe Test	Status/ Action
3.x.x									
3.x.x									
3.x.x									

K.61 Substantive Pass — Publication and Baseline Caution

This appendix intentionally preserves the distinction between the current CMMC Level 2 baseline and the broader NIST publication lifecycle. NIST SP 800-171 Revision 2 was withdrawn on May 14, 2024 and superseded by Revision 3. Current Department CMMC materials, however, continue to identify 110 NIST SP 800-171 Revision 2 requirements for Level 2, and the current CMMC Level 2 Assessment Guide Version 2.13 references the June 2018 NIST SP 800-171A assessment methods.

Accordingly, an MSP should not automatically replace a current CMMC Level 2 mapping with Revision 3 merely because Revision 3 is the current NIST publication. The applicable CMMC program materials and contract requirements must be checked at the time of use. Revision 3 can still inform modernization and future planning, but that is a separate exercise from documenting the current Level 2 assessment baseline.

K.62 Substantive Pass — Closing Perspective

Appendix K should function as the bridge between regulatory language and managed-service reality. The 110 requirements tell the organization what security outcomes must be implemented; the assessment guide explains how those outcomes are evaluated; the SSP and responsibility model explain the environment; and the MSP's operational records demonstrate what actually happens.

When Party ABC, Party EGH, and Party IJK can trace a requirement from official text to scoped asset, responsible party, implementation, recurring operation, evidence, interviewee, and safe test, CMMC preparation becomes much more disciplined. The cross-reference stops being a spreadsheet created for an assessor and becomes a management system for continuous readiness.

K.63 Final Regulatory Verification and Publication Note

This appendix is a teaching and operational cross-reference. It does not replace the authoritative NIST SP 800-171 Revision 2 publication, the current CMMC Level 2 Assessment Guide, 32 CFR part 170, applicable DFARS clauses, a solicitation or contract, or an organization's System Security Plan. The exact official requirement language and assessment objectives should be used when making a compliance or assessment determination.

Final verification on September 22, 2026 confirms that current Department CMMC materials identify Level 2 as using 110 security requirements from NIST SP 800-171 Revision 2. The Department also states that Phase II implementation, originally scheduled for November 10, 2026, was suspended on July 13, 2026, while Phase I self-assessment requirements remain in place. During the current pause, the Department states that it will enforce NIST SP 800-171 Revision 2 compliance through self-assessments and select government-led assessments.

The current CMMC Level 2 Assessment Guide, Version 2.13, states that Level 2 incorporates the security requirements in NIST SP 800-171 Revision 2. The guide uses the assessment methods examine, interview, and test. Accordingly, this appendix treats documentation, technical mechanisms, recurring activities, knowledgeable personnel, and safe demonstrations as distinct but complementary forms of assessment support.

NIST withdrew SP 800-171 Revision 2 on May 14, 2024 and superseded it with SP 800-171 Revision 3. That NIST publication lifecycle change does not, by itself,

replace the current CMMC Level 2 baseline described in Department CMMC materials. Organizations should distinguish modernization planning based on newer NIST publications from the specific requirements incorporated into their applicable CMMC and contractual obligations.

DFARS 252.204-7021 (NOV 2025) requires, when included and applicable, a current CMMC status at the required level for covered contractor information systems used in contract performance, annual affirmations of continuous compliance in SPRS for applicable CMMC UIDs, applicable flowdown, and successful closeout of a valid POA&M when the contractor has Conditional CMMC Status. These contractual requirements should be read together with the current CMMC program regulation and the specific contract.

Because the CMMC program is under active review as of this verification date, readers should recheck official Department CMMC resources, Acquisition.gov, 32 CFR part 170, and the applicable solicitation or contract before relying on this appendix for a live procurement or assessment.

K.64 Authoritative Sources Used for Final Verification

- NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations; NIST CSRC status page (withdrawn May 14, 2024; superseded by Revision 3).
- CMMC Assessment Guide - Level 2, Version 2.13, Department CMMC program resources.
- Current CMMC About and Resources & Documentation pages, Department CMMC program, verified September 22, 2026.
- DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025), Acquisition.gov.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program.

K.65 Final Publication Standard

For publication, the operational-focus labels in the 110-requirement matrix remain intentionally paraphrased teaching descriptions. They should not be quoted as the official NIST requirement text. The official NIST publication and current CMMC Assessment Guide remain the authoritative references for exact wording and assessment objectives. This distinction preserves the appendix's role as an MSP

implementation guide while avoiding confusion between instructional summaries and normative requirements.

Appendix L

Acronyms and Glossary

Detailed Teaching and Operational Edition

L.1 Purpose of This Appendix

CMMC work uses terminology from cybersecurity, federal contracting, NIST publications, cloud services, assessment practice, and managed services. The same word can also be used differently by a technician, an assessor, a contracting professional, and a customer executive. This appendix provides a practical teaching reference for the terminology used throughout this book.

The definitions below are written to help an MSP or defense contractor understand how the term is used operationally. They are not intended to replace a controlling statutory, regulatory, contractual, or standards definition. When an exact definition matters to a procurement, assessment, or legal obligation, the reader should consult the applicable authoritative source.

L.2 How to Use the Acronym List and Glossary

The acronym section is designed for quick lookup while reading the book. The glossary goes further by explaining why the term matters, how it appears in MSP operations, and where misunderstandings commonly occur. Party ABC and Party EGH are used as fictional defense-contractor customers, while Party IJK represents the MSP or external service provider.

L.3 Acronym Quick Reference

AC. Access Control

ATO. Authorization to Operate

AU. Audit and Accountability

C3PAO. Certified Third-Party Assessment Organization

CA. Security Assessment

CAGE. Commercial and Government Entity

CFR. Code of Federal Regulations

CIO. Chief Information Officer

CMMC. Cybersecurity Maturity Model Certification

CM. Configuration Management

CSP. Cloud Service Provider

CUI. Controlled Unclassified Information

DC3. Department of Defense Cyber Crime Center

DFARS. Defense Federal Acquisition Regulation Supplement

DIB. Defense Industrial Base

DoD. Department of Defense

EDR. Endpoint Detection and Response

ESP. External Service Provider

FCI. Federal Contract Information

FIPS. Federal Information Processing Standards

FAR. Federal Acquisition Regulation

GCC. Government Community Cloud

GCC High. Government Community Cloud High

GRC. Governance, Risk, and Compliance

IAM. Identity and Access Management

IA. Identification and Authentication

IR. Incident Response

ISSO. Information System Security Officer

MA. Maintenance

MFA. Multifactor Authentication

MP. Media Protection

MSP. Managed Service Provider

MSSP. Managed Security Service Provider

NARA. National Archives and Records Administration

NIST. National Institute of Standards and Technology

OSA. Organization Seeking Assessment

PE. Physical Protection

POA&M. Plan of Action and Milestones

PS. Personnel Security

RA. Risk Assessment

RMM. Remote Monitoring and Management

SC. System and Communications Protection

SI. System and Information Integrity

SIEM. Security Information and Event Management

SOC. Security Operations Center

SP. Special Publication

SPRS. Supplier Performance Risk System

SSP. System Security Plan

VPN. Virtual Private Network

L.4 Core CMMC and Federal Contracting Terms

CMMC. Cybersecurity Maturity Model Certification. A Department of Defense program used to assess whether contractors and subcontractors have implemented required cybersecurity protections for information and systems associated with DoD contracts. For an MSP, CMMC is not merely a documentation exercise; the services it operates may become part of the customer's assessed environment or evidence chain.

CMMC Level 1. The CMMC level associated with safeguarding Federal Contract Information using the applicable basic safeguarding requirements. An MSP supporting a Level 1 customer still needs clear scope, responsibility, and evidence even though the requirement set is smaller than Level 2.

CMMC Level 2. The CMMC level associated with protection of Controlled Unclassified Information and the current program's use of the 110 NIST SP 800-171 Revision 2 security requirements. The exact assessment requirement depends on the applicable solicitation or contract and current CMMC program rules.

C3PAO. A Certified Third-Party Assessment Organization authorized within the CMMC ecosystem to perform applicable CMMC assessments. A readiness consultant or MSP that helps prepare an organization is not automatically the independent assessor.

Organization Seeking Assessment (OSA). The organization whose environment and implementation are being evaluated for a CMMC status. In this book, Party ABC or Party EGH commonly fills this role.

Defense Industrial Base (DIB). The network of organizations that provide products and services supporting the Department of Defense. It includes large prime contractors, small businesses, subcontractors, technology providers, and many specialized service organizations.

DFARS. The Defense Federal Acquisition Regulation Supplement. DFARS clauses can create cybersecurity and reporting obligations for DoD contractors. MSP personnel should understand which contractual duties belong to the contractor and which technical activities the MSP has been engaged to support.

FAR. The Federal Acquisition Regulation, the principal set of rules governing acquisition by federal executive agencies. FAR and agency supplements such as DFARS are important because cybersecurity requirements may enter the contractor's environment through contract clauses.

32 CFR Part 170. The federal regulation establishing the CMMC Program. It should be distinguished from contract clauses that implement or reference CMMC requirements in procurements.

Flowdown. The process by which a prime contractor or higher-tier subcontractor passes applicable contractual requirements to subcontractors. An MSP should not assume a customer has no cybersecurity obligations simply because the MSP is not itself the prime contractor.

Affirmation. A required statement by an authorized organizational official regarding continuing compliance with applicable CMMC requirements when required by the current program and contract terms.

CMMC UID. A unique identifier associated with a CMMC status in the applicable government system. It helps connect the status to the information systems or assessment scope represented by that status.

SPRS. Supplier Performance Risk System. A DoD system used for supplier-related information, including applicable cybersecurity assessment and CMMC-related records. Contractors should control who is authorized to make submissions or affirmations.

Conditional CMMC Status. A time-limited status available under specified program conditions when permitted requirements remain on an authorized Plan of Action and Milestones. It is not the same as having no remediation obligations.

Final CMMC Status. A status reflecting satisfaction of the applicable requirements for the assessed level under the program rules, subject to continuing obligations such as affirmations and maintenance of the implementation.

L.5 Information Types and Scope

Federal Contract Information (FCI). Information provided by or generated for the government under a contract to develop or deliver a product or service to the government that is not intended for public release, subject to the applicable FAR definition and exclusions.

Controlled Unclassified Information (CUI). Information that requires safeguarding or dissemination controls pursuant to law, regulation, or government-wide policy but is not classified national-security information. CUI identification and handling should be based on authoritative marking, contract, registry, and information-owner guidance rather than an MSP guessing from file content alone.

CUI Registry. The National Archives and Records Administration resource that identifies CUI categories, subcategories, authorities, and handling-related information. It is an important reference when determining what kind of controlled information is involved.

Covered Contractor Information System. A contractual term used in DFARS cybersecurity clauses for an unclassified information system owned or operated by or for a contractor that processes, stores, or transmits covered defense information.

Security Protection Asset. A system or component that provides security functions or capabilities to the assessed environment. Depending on the architecture and current

scoping guidance, certain MSP-operated security services can affect assessment scope and evidence.

CUI Asset. An asset that processes, stores, or transmits CUI. Accurate identification of these assets is central to Level 2 scoping.

Specialized Asset. A category used in CMMC scoping for certain assets such as operational technology, Internet of Things, government-furnished equipment, restricted information systems, and test equipment under the conditions defined by current scoping guidance.

Contractor Risk Managed Asset. A current CMMC scoping concept for certain assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices.

Out-of-Scope Asset. An asset that does not meet the criteria for inclusion in the applicable CMMC assessment scope. An organization should be able to explain why the asset is outside the boundary rather than simply label it out of scope.

Data Flow. The path information follows among users, endpoints, servers, applications, cloud services, networks, providers, and external parties. CUI data-flow diagrams are important because scope cannot be understood from an asset inventory alone.

Assessment Boundary. The practical boundary around the systems, assets, services, people, and connections that are relevant to the assessment under the applicable CMMC scoping rules.

L.6 NIST and Assessment Terminology

NIST. National Institute of Standards and Technology. NIST publishes cybersecurity standards and guidance heavily used in federal cybersecurity programs.

NIST SP 800-171. A NIST Special Publication addressing protection of CUI in nonfederal systems and organizations. Current CMMC Level 2 program materials use the 110 security requirements in Revision 2, while NIST has separately published Revision 3.

NIST SP 800-171A. The assessment publication associated with assessing the security requirements in SP 800-171. Its assessment methodology underlies the examine, interview, and test approach used in CMMC Level 2 assessment guidance.

Security Requirement. A required security outcome or condition. A requirement should not be confused with the particular product used to implement it.

Assessment Objective. A specific determination used to evaluate whether the requirement is satisfied. One security requirement can have multiple assessment objectives.

Examine. An assessment method involving review and analysis of assessment objects such as policies, procedures, plans, configurations, records, or other artifacts.

Interview. An assessment method involving discussions with individuals who can explain how a security requirement is implemented and operated.

Test. An assessment method in which mechanisms or activities are exercised under defined conditions and actual behavior is compared with expected behavior.

Assessment Evidence. Information that supports an assessment determination. Evidence can include documents, configurations, logs, tickets, reports, records, demonstrations, and information obtained through interviews.

Objective Evidence. Evidence that is attributable and sufficiently reliable to support a conclusion about implementation rather than merely expressing an intention.

Evidence Index. A structured catalog connecting evidence artifacts to requirements, assessment objectives, systems, owners, dates, and storage locations.

Sampling. The selection of representative items for examination or testing rather than inspecting every possible object. Organizations should not assume that a sample hides inconsistent implementation; the sampled items need to represent the actual environment.

L.7 Governance, Documentation, and Remediation

System Security Plan (SSP). The document describing the system boundary, environment, implementation of security requirements, connections, roles, and other information necessary to understand how the organization protects the system. The SSP should describe reality rather than an aspirational future state.

Plan of Action and Milestones (POA&M). A structured remediation record identifying a deficiency, planned corrective action, responsibility, milestones, and completion. CMMC rules restrict how POA&Ms may be used for assessment status;

an ordinary internal remediation tracker should not automatically be treated as an authorized CMMC POA&M.

Gap Assessment. A readiness activity that compares the current implementation with applicable requirements and identifies missing or incomplete elements. A gap assessment is not the same as an independent certification assessment.

Readiness Assessment. A preparation exercise intended to determine whether an organization is likely to be able to demonstrate its implementation. The term should not be used in a way that falsely suggests a C3PAO assessment result.

Responsibility Matrix. A structured record showing which party owns, decides, implements, operates, produces evidence, maintains evidence, and participates in assessment for a security function or requirement.

Shared Responsibility. A condition in which multiple organizations contribute to the same security outcome. Shared responsibility does not mean responsibility is undefined; it means the division of work must be documented clearly.

Continuous Readiness. Maintaining the security implementation, documentation, evidence, personnel knowledge, and corrective-action process continuously rather than preparing only immediately before an assessment.

Corrective Action. An action taken to address a deficiency, finding, incident lesson, or process weakness and prevent or reduce recurrence.

Root Cause. The underlying condition or combination of conditions that enabled a problem. Root-cause analysis should go beyond identifying the technician or immediate event and examine process, technology, authorization, training, and governance factors.

Compensating Control. A safeguard used to reduce risk when the primary or expected implementation cannot be used. Whether a compensating approach satisfies a particular requirement must be evaluated against the actual requirement and assessment objectives; the term should not be used as a blanket exception.

L.8 MSP, MSSP, ESP, and Cloud Terminology

Managed Service Provider (MSP). A provider that performs recurring technology operations for customers, such as endpoint administration, identity, networks, backup, cloud administration, help desk, patching, or monitoring. An MSP may support CMMC implementation without becoming the customer's overall compliance owner.

Managed Security Service Provider (MSSP). A provider focused on recurring cybersecurity services such as SOC monitoring, SIEM, EDR/MDR, vulnerability management, incident response, or security engineering.

External Service Provider (ESP). A provider external to the organization that performs functions or provides services relevant to the organization's systems or security requirements. Current CMMC scoping guidance should be consulted to determine how a particular ESP affects scope and assessment.

Cloud Service Provider (CSP). A provider of cloud computing services. When cloud services process, store, or transmit CUI, the applicable contractual and security requirements must be evaluated carefully.

Shared Responsibility Model. The division of security duties between a cloud/service provider and the customer. The provider may secure underlying infrastructure while the customer remains responsible for identity, configuration, data, endpoints, or other layers.

GCC. Microsoft Government Community Cloud, a Microsoft 365 government cloud offering designed for eligible government-related organizations. Eligibility and suitability should be evaluated separately from CMMC compliance.

GCC High. A Microsoft government cloud environment designed for organizations with more restrictive U.S. government requirements. Deployment does not by itself make an organization CMMC compliant; configuration, scope, identity, operations, and evidence still matter.

Tenant. A logically separated cloud environment associated with an organization. Tenant configuration, administrative roles, logging, sharing, applications, and identity settings can be significant to CMMC implementation.

Service Principal. A non-human identity used by an application or service to access cloud resources. Service principals require governance because excessive privileges, unmanaged secrets, or abandoned integrations can create significant risk.

RMM. Remote Monitoring and Management. An MSP platform used to administer and monitor customer endpoints and systems. Because an RMM platform can have broad privileged reach, compromise of the RMM control plane or technician identity can become a multi-customer incident.

PSA. Professional Services Automation. An MSP platform commonly used for ticketing, customer records, service workflows, time entry, and operational

management. PSA records can become important evidence when they capture authorization and completed security work.

SOC. Security Operations Center. A team or function that monitors security events, investigates alerts, coordinates escalation, and supports incident response.

SIEM. Security Information and Event Management. Technology that collects and analyzes security-relevant event data from multiple sources. A SIEM contributes to logging and monitoring requirements but does not, by itself, prove that every related requirement is satisfied.

EDR. Endpoint Detection and Response. Endpoint security technology used to detect suspicious activity, investigate behavior, and support response actions such as isolation. Operational monitoring and response procedures are as important as deployment.

L.9 Identity, Access, and Security Operations Terms

Identity and Access Management (IAM). The policies, processes, and technologies used to create, authenticate, authorize, review, modify, and remove identities and access.

Multifactor Authentication (MFA). Authentication using more than one factor category. MFA is particularly important for privileged and remote access, but implementation details and applicable requirements must be evaluated against the current security requirement.

Least Privilege. Providing only the access necessary to perform assigned functions. Least privilege applies to users, administrators, applications, service accounts, and other identities.

Privileged Account. An account with elevated authority capable of security-sensitive administration. Privileged accounts should receive stronger governance, monitoring, and access controls than ordinary accounts.

Service Account. A non-human account used by a service, application, scheduled task, integration, or automated process. Service accounts should have defined ownership, purpose, privileges, credential management, and review.

Conditional Access. Policy-based access enforcement that considers conditions such as user, device, application, location, risk, or authentication strength. It is a technical mechanism, not a substitute for the underlying access-control requirement.

Zero Trust. A security architecture approach based on explicit verification, least privilege, and assumptions that trust should not be granted solely because a user or device is inside a traditional network boundary.

Security Baseline. An approved set of configuration settings and security expectations used as a starting point for systems or devices.

Configuration Drift. A condition in which a system's actual configuration moves away from its approved baseline, often because of manual changes, software updates, troubleshooting, or inconsistent deployment.

Vulnerability. A weakness that can potentially be exploited to compromise confidentiality, integrity, or availability.

Vulnerability Scan. An automated or semi-automated examination intended to identify known vulnerabilities or insecure conditions. Scan results need scope validation, prioritization, remediation, and rescan to become an effective vulnerability-management process.

Patch Management. The process of identifying, evaluating, testing, deploying, verifying, and documenting software and firmware updates.

Exception. An approved departure from a standard policy, configuration, or process. Exceptions should identify the reason, approver, duration, risk, compensating safeguards, and review or expiration.

L.10 Incident Response and Evidence Terms

Security Event. An observable occurrence in a system or network. An event can be benign, suspicious, or security relevant without necessarily becoming an incident.

Alert. A notification generated by a security mechanism or monitoring process indicating that defined conditions have been detected and require evaluation.

Security Incident. An occurrence that actually or potentially jeopardizes confidentiality, integrity, or availability or violates security policy. Contractual definitions and reporting thresholds may use more specific terminology.

Covered Cyber Incident. A DFARS-defined cyber incident that results in actual or potentially adverse effects on a covered contractor information system, covered defense information, or the contractor's ability to provide operationally critical support, subject to the controlling clause language.

Triage. The initial process of validating an alert or report, estimating severity and scope, identifying immediate risk, and deciding escalation and containment priorities.

Containment. Actions intended to limit the spread, impact, or continuing activity of an incident while preserving necessary evidence and business considerations.

Eradication. Actions that remove malicious artifacts, persistence, compromised credentials, vulnerable components, or other causes that could permit the incident to continue or recur.

Recovery. Restoring systems and services to trusted operation and validating that security controls and monitoring are functioning.

Chain of Custody. Documentation showing who collected, possessed, transferred, stored, or handled evidence and when. The required rigor depends on the investigation and intended use of the evidence.

Incident Chronology. A time-ordered reconstruction of events, observations, decisions, actions, and communications associated with an incident.

Indicator of Compromise (IOC). An observable artifact or condition that may indicate malicious activity, such as a hash, domain, IP address, account behavior, process, or persistence mechanism.

After-Action Report. A structured record of what occurred, how the organization responded, what worked, what failed, and what corrective actions should follow.

L.11 Cryptography, Network, and Data Protection Terms

Encryption. Transformation of data using cryptographic methods so that unauthorized parties cannot readily read it. Encryption can protect CUI at rest and in transit when implemented with the required cryptographic mechanisms.

FIPS-Validated Cryptography. Cryptographic modules validated under the applicable Federal Information Processing Standards validation program. A product merely advertising a standard algorithm is not necessarily the same as using a validated cryptographic module in the required manner.

Data at Rest. Data stored on media, endpoints, servers, databases, cloud storage, backups, or other persistent locations.

Data in Transit. Data moving across a network or communications channel between systems, services, users, or organizations.

Network Segmentation. Use of network architecture and controls to separate systems or security zones and restrict traffic among them. Segmentation can reduce scope and risk only when the separation is real, enforced, and documented.

Boundary Protection. Security controls at logical or physical communications boundaries that monitor, restrict, or protect traffic between environments.

VPN. Virtual Private Network. A technology for creating an encrypted network connection across an untrusted network. A VPN is one component of remote-access security and should be combined with identity, authorization, endpoint, and monitoring controls.

Split Tunneling. A remote-access configuration in which some traffic uses the protected tunnel while other traffic uses a separate network path. Applicable requirements may restrict split tunneling because it can bypass organizational monitoring or boundary protections.

Data Loss Prevention (DLP). Technology and processes intended to identify and control sensitive data movement. DLP can support CUI protection but requires accurate policy, labeling/context, tuning, investigation, and governance.

L.12 Operational Terms Used Throughout This Book

Operational Acceptance. A formal decision that a system, service, customer environment, or transition is sufficiently implemented, documented, monitored, and supportable to enter normal operations. It is distinct from CMMC certification.

Control Owner. The person or organizational function accountable for ensuring a security control or requirement is governed appropriately. The control owner may not be the technician who operates the mechanism.

Control Operator. The person or provider that performs recurring activities necessary for the control to function, such as reviewing alerts, patching endpoints, or managing accounts.

Evidence Producer. The person, process, or system that creates an artifact demonstrating implementation or operation.

Evidence Owner. The party responsible for maintaining and making the evidence available for the required purpose and retention period.

Evidence Custody. Responsibility for storing and protecting an evidence artifact. Custody can be held by an MSP even when the customer remains accountable for demonstrating the requirement.

Break-Glass Account. A tightly controlled emergency account used when ordinary administrative access is unavailable. It should have defined authorization, monitoring, credential protection, testing, and post-use review.

Runbook. A detailed operational procedure describing how a recurring or high-risk technical activity should be performed.

Playbook. A structured response or operational guide, often scenario-based, that coordinates actions, decisions, roles, and escalation.

Change Control. A process for requesting, evaluating, approving, implementing, documenting, and validating changes to systems and security configurations.

Operational Evidence. Records created through real operation, such as tickets, logs, reports, access reviews, restore tests, incident records, and change approvals.

Point-in-Time Evidence. Evidence showing the state of a system or configuration at a particular moment. It can be useful but may not demonstrate that a recurring process operates consistently.

Continuous Monitoring. Ongoing or recurring observation of security controls, systems, events, vulnerabilities, configuration, and other indicators to determine whether the security posture remains effective.

Technical Debt. Accumulated weaknesses, obsolete systems, deferred upgrades, unsupported configurations, or shortcuts that increase future operational and security cost.

Inherited Capability. A security capability supplied by another system or provider that contributes to the organization's implementation. The organization still needs to understand the dependency and maintain evidence of how it applies.

L.13 Frequently Confused Terms

CMMC Assessment vs. Gap Assessment. A CMMC assessment is performed under the applicable official assessment process. A gap assessment is a readiness activity used to identify deficiencies before an official assessment.

MSP vs. C3PAO. An MSP operates or supports technology. A C3PAO performs authorized independent assessments. A provider should not blur readiness support and independent assessment roles.

CUI vs. FCI. FCI and CUI are not interchangeable. CUI carries specific safeguarding or dissemination requirements and drives the Level 2 discussion in this book.

Policy vs. Evidence. A policy states what the organization requires. Evidence shows that the requirement has actually been implemented or operated.

Tool vs. Requirement. A security product can contribute to implementation, but the product name is not the requirement. The organization must connect the technology to the required outcome.

Compliance vs. Security. Compliance demonstrates satisfaction of defined requirements. Security is the broader practice of managing real threats and risk. Strong programs align the two rather than treating compliance as the entire security mission.

Backup vs. Recovery. A successful backup job does not prove recoverability. Recovery requires restoration and validation that the restored system or data can be trusted and used.

Alert vs. Incident. An alert is a signal requiring evaluation. An incident is a security occurrence that meets the organization's or applicable contractual definition and response criteria.

Owner vs. Operator. The party accountable for a requirement is not necessarily the party performing the technical work.

Evidence Producer vs. Evidence Owner. An MSP platform may create the record while the contractor needs the record for its assessment. Contracts and procedures should address access, retention, and transfer.

L.14 Party ABC, Party EGH, and Party IJK Glossary Example

Party ABC contracts with Party IJK to operate identity, endpoint security, SIEM, vulnerability management, and backup. ABC remains the Organization Seeking Assessment. Its SSP describes the environment and the division of responsibilities. Party IJK is an MSP and, for applicable services, may also be an External Service Provider.

A vulnerability alert from Party IJK's scanner is not itself remediation. It becomes part of an operational evidence chain when Party IJK validates the affected asset, opens a ticket, ABC or IJK makes the authorized remediation decision according to the responsibility model, the change is completed, and a rescan verifies the result.

Likewise, a SIEM dashboard is not the same as incident response. The SIEM may generate an alert; the SOC performs triage; the incident process determines whether escalation is required; authorized personnel decide containment; evidence is preserved; and ABC retains the records needed to demonstrate how the process operated.

L.15 Glossary Maintenance Guidance

The glossary should be reviewed whenever the Department changes CMMC terminology, NIST publications are incorporated into the program, DFARS clauses change, or major technologies introduce new operational terms. Definitions that have a controlling regulatory or contractual meaning should be reverified immediately before publication.

MSPs should also maintain a customer-specific vocabulary for terms that can be ambiguous. For example, 'administrator,' 'production,' 'CUI enclave,' 'security incident,' 'critical system,' and 'emergency change' should have a shared operational meaning so that customer and provider personnel make consistent decisions.

L.16 Closing Teaching Perspective

Terminology matters because CMMC work crosses technical, contractual, operational, and assessment boundaries. When the MSP and customer use the same words differently, responsibility gaps and evidence gaps appear quickly. A shared vocabulary allows Party ABC, Party EGH, and Party IJK to discuss scope, implementation, evidence, incidents, and assessment expectations with much greater precision.

This appendix should therefore be used as more than a list of abbreviations. It is a translation layer between the language of federal cybersecurity requirements and the language of everyday managed-service operations.

L.17 Deepening Pass — CMMC Assessment Scope Terminology

In-Scope Asset. An asset included in the assessment boundary under the applicable CMMC scoping criteria. Inclusion should be supported by the asset's role, connectivity, information handling, or security function rather than by convenience.

Asset Inventory. A maintained record of systems, devices, applications, virtual resources, cloud resources, and other assets relevant to the environment. For CMMC work, inventory quality directly affects scoping, vulnerability management, configuration management, and evidence.

CUI Enclave. A commonly used operational term for an intentionally bounded environment designed to contain CUI processing, storage, and transmission. The term itself does not create compliance; the actual architecture, connections, people, providers, and controls determine the implementation.

Security Protection Data. Information generated or used by security capabilities, such as logs, alerts, configurations, authentication records, vulnerability findings, and security-management information. Its relationship to scope should be evaluated under current CMMC guidance.

External Connection. A connection between the assessed environment and another system, network, service, organization, or security boundary. External connections should be authorized, documented, protected, and represented accurately in diagrams.

Interconnection. A persistent or controlled connection that allows systems or environments to exchange information or services. Interconnections can affect CUI flow and scope even when the connected system does not directly host a CUI repository.

Logical Boundary. A boundary created through technical controls such as network segmentation, identity policy, tenant separation, firewall rules, or application architecture.

Physical Boundary. A facility, room, cage, rack, or other physical separation used to control access to systems and media.

Scope Validation. The process of comparing diagrams, inventories, data flows, provider relationships, configurations, and actual operations to determine whether the documented assessment boundary reflects reality.

L.18 Deepening Pass — Cloud and Government Cloud Terminology

Commercial Cloud. A generally available cloud service environment offered to commercial customers. Whether it is suitable for a particular CUI workload depends on contractual, security, service, and data-handling requirements.

Government Cloud. A cloud service designed for eligible government or government-related customers and particular regulatory requirements. The phrase is broad and should not be treated as proof that every service satisfies every defense-contract requirement.

FedRAMP. Federal Risk and Authorization Management Program. FedRAMP provides a standardized approach for security assessment and authorization of cloud services used by federal agencies. Its relationship to a defense contractor's cloud use must be evaluated against the applicable DFARS and contract requirements.

FedRAMP Moderate. A FedRAMP impact-level baseline commonly discussed when evaluating cloud services for CUI-related use. An MSP should verify the exact contractual requirement and the service's authorization/equivalency status rather than rely on marketing language.

FedRAMP Moderate Equivalent. A concept relevant to certain DFARS cloud-service requirements. Equivalency is not established merely because a vendor states that it follows similar controls; the applicable DoD criteria and contract language must be evaluated.

Microsoft 365 Government. A family of Microsoft cloud offerings designed for government-related customers. The specific environment—rather than the word 'government' alone—matters when determining service availability, data location, eligibility, and contractual suitability.

Azure Government. Microsoft's government-focused Azure cloud environment. Its architecture and service availability differ from commercial Azure and should be documented accurately when it supports a CUI environment.

Tenant-to-Tenant Migration. The movement of identities, mail, files, applications, configurations, or other cloud resources from one tenant to another. For CMMC customers, migration planning should preserve security settings, evidence, data protection, and responsibility continuity.

Cloud Audit Log. A provider-generated record of identity, administrative, application, file, security, or other cloud activity. Audit availability, licensing,

retention, and export capabilities should be understood before an incident or assessment.

Application Consent. Authorization allowing an application to access cloud data or functions. Excessive or malicious consent can create persistent access even when a user's password is changed.

Delegated Administration. A model in which a customer authorizes a provider or partner to perform selected administrative functions. The MSP should limit delegated privileges and retain evidence of authorization and use.

L.19 Deepening Pass — Contract, Flowdown, and Supplier Terms

Prime Contractor. An organization holding a direct contract with the government. Prime contractors frequently impose applicable requirements on subcontractors through contractual flowdown.

Subcontractor. An organization performing work under a higher-tier contractor rather than directly for the government. CMMC and safeguarding requirements can apply through the subcontract relationship.

Subcontractor Flowdown. The contractual passing of specified requirements to lower-tier organizations. The recipient should review the actual clause and scope rather than rely solely on a customer's informal statement.

Solicitation. A government request for offers, proposals, bids, or quotations. Cybersecurity and CMMC requirements can appear at the solicitation stage and affect whether an organization is eligible to compete.

Contract Clause. A legally operative provision incorporated into a contract. Technical teams should understand that a framework document, assessment guide, and contract clause serve different purposes.

Contracting Officer. A government official with authority to enter into, administer, or terminate contracts and make related determinations within delegated authority. MSP personnel should not assume they can make contractual interpretations on the customer's behalf.

Prime/Sub Relationship. The commercial and contractual relationship between a prime contractor and a subcontractor. Responsibility for CUI and CMMC should be documented rather than inferred from company size or contract tier.

Supplier Due Diligence. Evaluation of a provider's security, contractual, technical, operational, and evidence capabilities before entrusting it with services that affect CUI or security requirements.

Third-Party Risk. Risk introduced by vendors, providers, subcontractors, software, integrations, supply chains, and other external dependencies.

Service-Level Agreement (SLA). A contractual or service-management statement defining expected service performance such as response time, availability, or support. An SLA does not by itself define CMMC responsibility.

Statement of Work (SOW). A document describing services, deliverables, responsibilities, and performance expectations. For an MSP supporting CMMC, the SOW should align with the responsibility matrix and actual service boundary.

L.20 Deepening Pass — Evidence and Assessment Operations

Evidence Repository. A controlled location where assessment and readiness artifacts are indexed and maintained. It should protect sensitive information and support controlled assessor access.

Evidence Package. A curated group of artifacts supporting a particular requirement, family, system, or assessment objective.

Evidence Freshness. The degree to which an artifact reflects the current assessed environment and an appropriate operating period.

Evidence Traceability. The ability to connect an artifact to a requirement, assessment objective, system, responsible party, source, and period of operation.

Evidence Validation. Review performed to determine whether an artifact actually supports the intended assessment objective and matches the documented implementation.

Artifact. A document, export, screenshot, ticket, report, configuration record, log, diagram, or other item used as evidence.

Screenshot Evidence. A captured image of a configuration or system state. Screenshots can be useful but should include enough context to identify what is being shown and should not replace stronger exported or recurring evidence when available.

Interview Readiness. The state in which personnel understand their actual responsibilities and can explain the implementation accurately without relying on memorized scripts.

Test Readiness. Preparation to demonstrate a security mechanism or activity safely and consistently with the documented production implementation.

Evidence Gap. A condition in which implementation may exist but sufficient evidence has not been identified, retained, or connected to the assessment objective.

Implementation Gap. A condition in which the required security outcome is missing or incomplete. An implementation gap is more serious than merely having difficulty locating evidence.

Documentation Gap. A mismatch or omission in policy, procedure, SSP, diagram, responsibility matrix, or other documentation relative to the actual implementation.

Assessment Readiness. The ability to demonstrate the current implementation through coherent documentation, evidence, knowledgeable personnel, and safe testing.

Evidence Period. The span of time represented by operational records. Recurring requirements often benefit from evidence across an operating period rather than a single moment.

L.21 Deepening Pass — CUI Handling and Data Lifecycle Terms

CUI Lifecycle. The sequence through which CUI is received or created, accessed, used, stored, transmitted, shared, archived, and ultimately disposed of.

CUI Repository. A system or location where CUI is stored, such as a file server, document library, database, application, endpoint, or approved cloud service.

CUI Transmission. Movement of CUI between systems, users, services, or organizations. Transmission protections should reflect the applicable security requirements and approved architecture.

CUI at Rest. CUI stored on persistent media or storage services. Encryption, access control, backup protection, and media management can all affect its protection.

CUI in Transit. CUI moving through a network or communication channel. Secure protocols, cryptography, boundary controls, and approved destinations are important considerations.

CUI Marking. The application of required markings or dissemination controls to CUI under applicable government-wide CUI policy. MSPs should not invent markings when authoritative direction is absent.

Authorized Recipient. A person or organization permitted to receive the information under applicable authorization, contract, policy, and need-to-know conditions.

Data Disposition. The controlled retention, transfer, return, sanitization, destruction, or other final handling of information when it is no longer required.

Secure Sanitization. A process that renders data on media infeasible to access for a given level of effort, using methods appropriate to the media and applicable requirements.

Media Destruction. Physical destruction of media using an approved method when reuse is not intended or sanitization requirements call for destruction.

Data Spillage. The placement or transmission of sensitive information into a system, location, or channel not authorized for that information. Response should focus on containment, preservation, notification, and approved remediation rather than simply deleting the visible copy.

L.22 Deepening Pass — Licensing, Tooling, and Operational Ownership

License Owner. The organization contractually holding or controlling a software subscription or license. License ownership should be distinguished from administration and operational responsibility.

License Administrator. The person or provider that assigns, configures, renews, or manages software licenses. The administrator may not own the commercial agreement.

Security Feature Licensing. The license level required to enable a security capability such as advanced logging, retention, endpoint protection, identity governance, or conditional access. MSP designs should verify that required features are actually licensed.

License Dependency. A condition in which a security control or evidence source depends on a particular subscription level. Downgrading or expiration can silently remove capability or historical evidence.

Tool Ownership. Responsibility for the commercial and administrative control of a platform. A customer-owned SIEM and an MSP-owned SIEM can create different evidence, retention, and offboarding considerations.

Operational Ownership. Responsibility for recurring execution of a service or security process. Operational ownership should be explicit even when the technology is customer-owned.

Administrative Plane. The management interface, APIs, privileged identities, automation, and control functions used to administer a technology environment.

Control Plane. The mechanisms that configure and direct how a platform or service operates. Compromise of an MSP control plane can affect many customer environments.

API Token. A credential used by software to access an application programming interface. API tokens should have defined ownership, least privilege, secure storage, rotation, monitoring, and revocation.

Secret Rotation. Replacement of passwords, keys, tokens, certificates, or other secrets on a planned or incident-driven basis.

Subscription Transfer. The controlled movement of commercial or administrative responsibility for a service from one organization to another during onboarding, offboarding, acquisition, or provider transition.

L.23 Deepening Pass — Continuous Readiness and Operational Assurance

Operational Assurance. Ongoing confidence, supported by evidence, that systems and security processes continue to operate as intended.

Control Health. The current operating condition of a security mechanism or process, including coverage, configuration, errors, exceptions, and monitoring status.

Security Tool Health. Evidence that a security technology such as EDR, SIEM, backup, vulnerability scanning, or identity protection is connected, licensed, updated, reporting, and functioning.

Coverage Gap. An asset, identity, service, log source, location, or process that should be protected or monitored but is not currently covered.

Drift Review. A recurring comparison between approved configuration and actual configuration to identify unauthorized or unintended changes.

Exception Register. A maintained record of approved departures from normal security requirements, including owner, rationale, compensating safeguards, approval, expiration, and review.

Remediation Tracker. An operational record of deficiencies and corrective actions. It should not automatically be labeled a CMMC POA&M unless it meets the applicable program conditions.

Control Validation. A review or test confirming that a safeguard continues to produce its intended security result.

Readiness Review. A periodic review of implementation, evidence, responsibility, personnel knowledge, and unresolved gaps.

Operational Acceptance Criteria. Defined conditions that must be satisfied before a system, service, or transition is accepted into normal operation.

Security Debt. Accumulated security weaknesses or deferred corrective actions that increase operational risk and make future compliance or assessment more difficult.

Evidence Debt. Accumulated failure to retain, organize, or connect operational evidence even when technical work may have occurred.

Assessment Debt. The combined effect of implementation, documentation, evidence, and knowledge gaps that makes an organization progressively harder to assess successfully.

L.24 Deepening Pass — Incident Reporting and Communication Terms

Discovery Time. The point at which an organization determines that a cyber incident has been discovered for purposes of its applicable process or contractual obligation. Exact contractual meaning should be determined from the controlling clause.

Rapid Reporting. The reporting obligation defined by applicable DFARS cyber-incident language. The technical team should preserve discovery time and facts so the contractor can make and support the required reporting decision.

Reportable Incident. An incident meeting a defined reporting threshold under a contract, regulation, policy, insurer requirement, or other obligation. Not every security alert is reportable.

Initial Incident Report. The first formal report submitted under an applicable reporting process. Early reports may contain known facts and unresolved questions; accuracy is more important than unsupported certainty.

Supplemental Report. Additional information submitted after the initial report when the reporting process permits or requires updates.

Situation Report. A concise operational update describing confirmed impact, containment, unresolved questions, decisions required, and the next planned update.

Communication Tree. A predefined sequence of internal and external contacts used to coordinate incident communications.

Alternate Communication Channel. A trusted method of communication used when normal email, collaboration, identity, or MSP systems may be compromised.

Need to Know. A principle limiting sensitive information to individuals who require it to perform authorized duties. Incident communications should avoid unnecessary distribution.

Executive Status Update. A management-focused incident summary emphasizing business impact, confirmed facts, decisions, risk, and next actions rather than raw technical telemetry.

L.25 Deepening Pass — People and Responsibility Terminology

System Owner. The organizational role accountable for a system and its business use, security expectations, and lifecycle decisions.

Information Owner. The person or organization responsible for determining appropriate use, protection, sharing, and disposition of information.

Risk Owner. The person with authority to accept, reject, mitigate, or escalate a particular organizational risk.

Technical Lead. The person directing technical investigation or implementation activities. Technical leadership does not automatically confer authority to make business, contractual, or legal decisions.

Incident Commander. The person coordinating the overall incident response process, assignments, priorities, communications, evidence, and decision flow.

Decision Authority. The person or role authorized to approve a consequential action such as system shutdown, exception, external reporting, risk acceptance, or return to service.

Authorized Administrator. An individual explicitly approved to perform defined administrative functions.

Readiness Consultant. A person or organization assisting with preparation, gap analysis, documentation, evidence, or remediation. Readiness assistance should be distinguished from independent assessment.

Independent Assessor. An assessor who performs an authorized evaluation under the applicable assessment process and independence requirements.

Subject Matter Expert (SME). A person with specialized knowledge of a technology, process, requirement, or business function who can support implementation or assessment explanation.

L.26 Deepening Pass — A Practical Vocabulary for Party IJK

Party IJK should incorporate these terms into service documentation rather than treating the glossary as book-only material. Tickets can identify decision authority and evidence producer. Onboarding records can identify license owner and operational owner. Incident procedures can distinguish an alert, security incident, covered cyber incident, situation report, and reporting decision. Assessment records can distinguish an evidence gap from an implementation gap.

This vocabulary becomes especially important when Party IJK supports multiple customers. Party ABC may own its Microsoft tenant while Party IJK administers it. Party EGH may use an MSP-owned SIEM. The technical services can look similar while ownership, evidence custody, licensing, offboarding, and assessment responsibilities differ substantially.

L.27 Deepening Pass — Glossary Governance

The glossary should have an owner and review cycle. Terms tied directly to CMMC, DFARS, NIST, CUI policy, cloud-service requirements, or assessment methodology should be checked against authoritative sources before each major book revision.

Operational terms created for this book should remain consistent across chapters and appendices.

When a regulatory term has a precise official definition, the teaching definition should explain the concept without silently changing the controlling meaning. Where necessary, the book should tell the reader to use the official source for an actual contractual or assessment determination.

L.28 Deepening Pass — Closing Perspective

A mature CMMC program depends on shared language. The customer, MSP, compliance team, assessor, contracting personnel, executives, and technicians may approach the same environment from very different professional backgrounds. A glossary reduces the chance that those groups use the same word to mean different things.

The purpose of Appendix L is therefore not simply to help a reader remember what an acronym stands for. Its deeper purpose is to create a common operational vocabulary that connects cybersecurity requirements to managed-service work, responsibility, evidence, assessment, and continuous readiness.

L.29 Substantive Pass — A–Z Operational Reference

This section consolidates additional terms that appear across the book and places them in an operational context. The purpose is not to duplicate every earlier definition, but to make Appendix L useful when a reader enters the book at any chapter and needs a quick explanation of the language used by contractors, MSPs, assessors, security teams, and contracting personnel.

Affirming Official. The organizational official responsible for making an affirmation of continuous compliance when required by the CMMC program. This is an organizational accountability role; an MSP technician should not assume authority to make the affirmation for a customer.

Allowlisting. A security approach in which only explicitly authorized software, applications, commands, connections, or other objects are permitted. It can support least functionality and application-control objectives.

Asset Category. A classification used to explain how an asset relates to the CMMC assessment scope. The classification should reflect the current scoping guidance and the asset's real function.

Authentication Factor. A category of evidence used to authenticate an identity, commonly something known, possessed, or inherent. MFA requires distinct factor categories rather than simply two passwords.

Authorization. The decision that an authenticated identity is permitted to perform a function, access a resource, or receive information. Authentication answers who the identity is; authorization determines what it may do.

Baseline Configuration. An approved, documented configuration used as a reference state for systems. A baseline becomes operationally useful when changes and drift can be compared against it.

Business Continuity. The capability to sustain or restore essential business operations during disruption. It overlaps with, but is not identical to, incident response and disaster recovery.

Change Advisory Board. A governance mechanism used by some organizations to review and approve significant changes. The name of the body is less important than having defined authorization and security-impact review.

Compromise. A condition involving unauthorized disclosure, modification, destruction, loss, or other violation of system or information security. Applicable contract clauses may provide controlling definitions.

Configuration Item. A managed component whose configuration is tracked, such as a server, firewall, endpoint, application, tenant setting, or security platform.

Corrective Action Plan. A structured plan for resolving a deficiency or weakness. It may be an internal management artifact and should not automatically be treated as a formal CMMC POA&M.

Cyber Incident. A cybersecurity event that meets the applicable incident criteria. Under DFARS 252.204-7012, specific reporting obligations apply when the clause's conditions are met.

Defense-in-Depth. The use of multiple complementary safeguards so failure of one layer does not leave the system without protection.

Deny by Default. A security model in which access or network communication is blocked unless explicitly permitted. This is stronger than attempting to identify and block every undesirable action individually.

Disaster Recovery. The technical and operational process for restoring systems, infrastructure, and data after a major disruption.

Encryption Key. Cryptographic material used by an algorithm to encrypt, decrypt, sign, verify, or otherwise protect information. Key generation, storage, access, rotation, backup, and destruction require governance.

Escalation. Transfer of an issue, alert, incident, risk, or decision to a person with greater expertise or authority. Effective escalation criteria prevent technicians from making decisions outside their authority.

Exception Approval. Documented authorization for a defined departure from a standard requirement or baseline. It should identify scope, rationale, risk, compensating safeguards, approver, and expiration or review date.

External System. A system outside the organization's authorization or control boundary. Use of an external system for CUI should be governed by applicable requirements and organizational authorization.

Forensic Image. A controlled copy of digital media or data created for forensic examination. Collection methods should preserve integrity and necessary metadata when forensic use is anticipated.

Hash. A cryptographic digest used to help verify data integrity or identify known files. Hash values can be useful in evidence handling and incident investigation.

Incident Severity. An organizational classification reflecting factors such as impact, scope, sensitivity, operational disruption, and urgency. Severity should guide response priority but should not replace contractual reporting criteria.

Least Functionality. The principle of configuring systems to provide only essential capabilities and restricting unnecessary functions, ports, protocols, services, and software.

Log Retention. The period and method for retaining audit and security records. Retention should be sufficient for applicable security, assessment, investigation, contractual, and business needs.

Malicious Code. Software or code designed to perform unauthorized or harmful actions. Protection includes prevention, detection, updating, scanning, investigation, and response.

Network Diagram. A representation of system components, network zones, connections, security boundaries, and relevant external services. For CMMC, the diagram should align with the documented assessment scope.

Privileged Function. A security-sensitive operation requiring elevated authority, such as changing system security settings, managing identities, or altering audit configuration.

Recovery Point Objective (RPO). The maximum targeted amount of data loss measured in time. RPO is a business continuity concept and should not be confused with evidence that backups actually restore.

Recovery Time Objective (RTO). The targeted time for restoring a system or service after disruption. An RTO is a planning objective, not proof of recovery capability.

Residual Risk. Risk remaining after safeguards and corrective actions are applied. Acceptance of residual risk should be made by an authorized risk owner.

Return to Service. The controlled decision to restore a system to normal production use after maintenance, recovery, or incident response. Validation should confirm that required security capabilities are functioning.

Risk Acceptance. A documented decision by an authorized person to accept identified risk. An MSP can explain technical risk but should not silently accept organizational risk for the customer.

Security Architecture. The design of security boundaries, identities, trust relationships, networks, applications, data flows, monitoring, and safeguards as an integrated system.

Security Configuration. A setting or combination of settings that affects a system's security behavior.

Security Control. A safeguard or countermeasure intended to protect confidentiality, integrity, availability, or another security objective. In CMMC discussions, the precise terminology of the applicable NIST/CMMC source should be preserved.

Security Incident Ticket. An operational record used to document investigation, decisions, actions, evidence, communications, and closure associated with an incident.

Security Requirement Family. A grouping of related NIST SP 800-171 requirements, such as Access Control, Incident Response, or System and Information Integrity.

System Boundary. The defined limits of a system, including relevant components, services, interfaces, and connections. Boundary accuracy is essential to the SSP and assessment scope.

System Hardening. The process of reducing attack surface through secure configuration, removal or restriction of unnecessary functionality, and application of approved security settings.

System of Record. The authoritative source used for a particular class of information, such as the PSA for service tickets or IAM platform for current group membership.

Threat. A circumstance or actor capable of adversely affecting systems or information through unauthorized access, destruction, disclosure, modification, or denial of service.

Vulnerability Remediation. The process of correcting or mitigating a vulnerability, validating the result, and documenting closure or an authorized exception.

L.30 Substantive Pass — CMMC Status and Assessment Terms

Level 1 Self-Assessment. The CMMC Level 1 assessment path based on the applicable basic safeguarding requirements for FCI and current program rules.

Level 2 Self-Assessment. A Level 2 assessment path used when the applicable solicitation or contract requires Level 2 self-assessment rather than a C3PAO assessment.

Level 2 C3PAO Assessment. A Level 2 certification assessment conducted by an authorized C3PAO when that assessment type is required.

Level 3 DIBCAC Assessment. The Level 3 assessment path involving the Defense Industrial Base Cybersecurity Assessment Center under the applicable CMMC program requirements.

Current CMMC Status. A CMMC status that satisfies the applicable age, affirmation, and continuing-compliance conditions defined in the controlling CMMC/DFARS requirements.

Final Level 2 Status. A final Level 2 status achieved under the applicable assessment path and current program rules. Current DFARS language treats Final Level 2 statuses as having a three-year assessment age limit, with annual affirmation conditions.

Conditional Level 2 Status. A Level 2 status available when the applicable conditions for use of a valid POA&M are met. Current DFARS language treats a Conditional Level 2 status as not older than 180 days and subject to continuous-compliance and affirmation conditions.

Annual Affirmation. The recurring affirmation of continuous compliance required by current CMMC/DFARS rules for applicable statuses. It should be supported by ongoing operational knowledge rather than treated as a ceremonial annual signature.

CMMC Status Date. The date associated with the assessment/status from which applicable currency periods are measured.

Assessment Result. The documented outcome of an assessment. Readiness teams should not describe an internal gap review as an official CMMC assessment result.

L.31 Substantive Pass — Scoping Terms That Require Precision

The current Level 2 scoping guide distinguishes CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and out-of-scope assets. These categories are not interchangeable labels. The asset inventory and network diagram should support the organization's categorization and allow an assessor to understand how the environment actually processes, stores, transmits, or protects CUI.

CUI Asset — Operational Meaning. An asset that processes, stores, or transmits CUI. Current Level 2 scoping guidance places CUI Assets in the assessment scope and subjects them to the applicable Level 2 requirements.

Security Protection Asset — Operational Meaning. An asset providing security functions or capabilities to the assessed environment. A SIEM, identity platform, security-management system, or provider-operated security service can become relevant because it protects the assessed environment even when it does not serve as a CUI repository.

Security Protection Data — Operational Meaning. Security-relevant information stored or processed by Security Protection Assets and used to protect the assessed

environment. Examples can include configurations and other security information whose disclosure could aid an attacker.

Contractor Risk Managed Asset — Operational Meaning. An asset that can, but is not intended to, process, store, or transmit CUI because organizational policy, procedures, and practices are used to prevent that use. The exact current scoping conditions should be verified rather than inferred from the name.

Specialized Asset — Operational Meaning. An asset falling into a specialized category recognized by current CMMC scoping guidance. Specialized status does not mean the asset can be ignored; the organization still has documentation and risk-management responsibilities.

Out-of-Scope Asset — Operational Meaning. An asset meeting the current criteria for exclusion from the CMMC assessment scope. Network location alone does not necessarily determine whether an asset is out of scope.

L.32 Substantive Pass — DFARS Cyber Incident Terms

Incident terminology deserves special care because operational shorthand can have contractual consequences. DFARS 252.204-7012 currently defines 'rapidly report' as reporting within 72 hours of discovery of a cyber incident. The clause also contains requirements concerning review for evidence of compromise and other incident-related obligations. The contractor should make reporting decisions using the controlling clause and qualified contractual/legal guidance where appropriate; the MSP's role is to provide timely, accurate technical facts and preserve the evidence needed for that decision.

72-Hour Reporting Window. The rapid-reporting timeframe stated in current DFARS 252.204-7012 for applicable cyber incidents. Incident procedures should capture discovery time and escalation promptly.

Preservation. The controlled retention of images and relevant monitoring/packet-capture data associated with a reported incident for the period required by the applicable clause.

Malicious Software Submission. A DFARS-related process that may apply when malicious software is discovered and isolated in connection with a reportable cyber incident. The current clause and DoD reporting instructions should govern the actual submission.

Damage Assessment Support. Technical information, systems, or access that may be required to support DoD analysis of the effect of a reported cyber incident under applicable contract terms.

L.33 Substantive Pass — Terms That Should Never Be Used Casually

Several phrases sound harmless in everyday IT conversation but can create confusion in a CMMC program. The following distinctions should be taught explicitly to MSP technicians, customer personnel, and readiness teams.

Certified. Do not describe a customer, product, technician, or MSP as 'CMMC certified' unless the statement accurately reflects the applicable official status and entity. Products do not become CMMC-certified simply because they are used in a certified environment.

Compliant. Avoid using 'compliant' as a casual synonym for 'we installed the tool.' Compliance conclusions depend on the applicable requirements, scope, implementation, evidence, and assessment or affirmation context.

FedRAMP Approved. Use precise authorization terminology. A cloud service's FedRAMP status should be verified through authoritative information rather than inferred from vendor marketing.

CMMC Ready. A useful informal readiness phrase only when its meaning is defined. It should not imply that an independent assessment has already occurred.

Out of Scope. A scoping conclusion that should be supported by current CMMC scoping criteria and architecture. It is not a label used merely because the organization would prefer not to assess an asset.

Compensating Control. Do not use the phrase as a universal waiver. The organization must determine whether the proposed implementation satisfies the actual requirement and applicable assessment objectives or whether formal treatment is required.

Inherited. Do not assume that using a cloud or MSP means the customer has no responsibility. Inheritance should identify exactly what capability is supplied, what evidence supports it, and what responsibilities remain with the customer.

L.34 Substantive Pass — Glossary Consistency Rules for the Book

For the remainder of this book and its appendices, 'customer' refers to the defense contractor or other organization receiving the managed service unless context states otherwise. 'MSP' refers to the provider performing recurring managed IT services; 'MSSP' is used when the service is specifically security-focused; and 'ESP' is used when discussing the formal CMMC concept of an external provider relevant to the assessed environment.

The word 'owner' should identify accountability or authority, while 'operator' identifies the party performing recurring work. 'Evidence producer' identifies who or what creates the artifact, and 'evidence owner' identifies the party responsible for maintaining or presenting it. These roles can be held by different parties.

The word 'assessment' should be qualified whenever ambiguity is possible. The book distinguishes gap assessment, readiness review, self-assessment, C3PAO assessment, and DIBCAC assessment. A readiness exercise should never be presented as though it produced an official CMMC status.

The word 'requirement' refers to the applicable security requirement or contractual obligation. A product, license, configuration, policy, screenshot, or ticket may support the requirement, but none of those artifacts should be described as the requirement itself.

L.35 Substantive Pass — Party ABC / EGH / IJK Responsibility Vocabulary

Consider Party ABC using Party IJK for managed identity. ABC is the organizational owner of the access policy and decides which employees require privileged access. Party IJK is the operator that provisions the account and enforces the approved configuration. The IAM platform is an evidence producer because it creates authentication and group-membership records. Party IJK's PSA is another evidence producer because it records authorization and implementation. ABC may remain the evidence owner for the assessment package even though the original records reside in provider systems.

Party EGH may use a different commercial model in which it owns the SIEM subscription but Party IJK operates the service. In that arrangement, tool ownership and operational ownership are separate. During offboarding, EGH may retain direct

access to historical logs while Party IJK transfers procedures, open investigations, service documentation, and provider-held evidence.

These distinctions are why the glossary repeatedly separates ownership, administration, operation, evidence production, evidence custody, and decision authority. They prevent a contract phrase such as 'managed security' from becoming an undefined transfer of all cybersecurity responsibility.

L.36 Substantive Pass — Reference Checklist for Readers

When encountering an unfamiliar term elsewhere in the book, the reader should ask four questions. First, is this an official regulatory, contractual, NIST, or CMMC term whose controlling definition must be checked? Second, is it an operational term used to explain how an MSP performs work? Third, does the term assign responsibility or authority? Fourth, does the term affect scope, evidence, assessment, or incident reporting? Those questions help determine how much precision is required.

A technician can often work safely with an operational definition. A contracting decision, assessment determination, CUI categorization, incident-reporting decision, or CMMC status statement requires the authoritative source and the current version of the applicable requirement.

L.37 Substantive Pass — Final Teaching Perspective Before Editorial Review

The strongest purpose of Appendix L is to keep language from becoming a hidden source of implementation failure. A customer may say 'the MSP owns security' while meaning that the MSP operates several tools. An MSP may say 'the customer is compliant' while meaning that its managed endpoints have the expected configuration. An executive may say 'everything is in GCC High' while overlooking local endpoints, backups, support tools, external providers, and identity administration.

Precise vocabulary forces those statements to become testable. Who owns the decision? Which system is in scope? Where does CUI travel? Which provider operates the safeguard? Which record proves it? Who can explain it to an assessor? Which contractual definition controls? Once those questions are answered, terminology becomes an operational control rather than a publishing convenience.

L.38 Final Regulatory Verification and Publication Note

This glossary is an instructional and operational reference. Where a term has a controlling definition in 32 CFR part 170, the FAR, DFARS, NIST publications, the CMMC Assessment Guide, or current CMMC scoping guidance, that authoritative definition governs. The explanatory definitions in this appendix are intended to help readers understand how the terminology appears in managed-service operations; they do not replace the controlling source.

Final verification on September 22, 2026 confirms that current Department CMMC materials describe Level 2 self-assessment as using the 110 security requirements in NIST SP 800-171 Revision 2, with assessment every three years and annual affirmation. The Department also states that CMMC implementation is paused in Phase I following the July 13, 2026 suspension of Phase II. Readers should therefore distinguish the current program implementation posture from the underlying obligation to protect covered information.

Current DFARS 252.204-7021 (NOV 2025) defines a current Conditional Level 2 status as not older than 180 days and a current Final Level 2 status as not older than three years, subject to the applicable continuous-compliance and affirmation conditions. The clause also defines annual affirmation currency as not older than one year.

Current DFARS 252.204-7012 (MAY 2024) defines rapidly report as within 72 hours of discovery of an applicable cyber incident. The clause also requires preservation and protection of images of known affected systems and relevant monitoring or packet-capture data for at least 90 days from submission of the cyber incident report, and addresses malicious-software submission when applicable.

NIST SP 800-171 Revision 2 was withdrawn on May 14, 2024 and superseded by Revision 3. The current CMMC program materials nevertheless continue to use the 110 Revision 2 security requirements for Level 2. The book therefore uses Revision 2 terminology where discussing the present CMMC Level 2 baseline while recognizing Revision 3 as the current NIST publication.

L.39 Final Terminology Consistency Standard

Throughout this book, C3PAO means CMMC Third-Party Assessment Organization when referring to the formal term used in 32 CFR part 170. OSA means Organization Seeking Assessment. MSP and MSSP describe managed-service operating roles,

while ESP is used when the formal CMMC external-service-provider concept is relevant. These terms should not be substituted for one another merely because the same company can occupy more than one role.

The book consistently distinguishes ownership from operation. The customer or OSA may remain accountable for a requirement while Party IJK implements or operates a technical capability. The evidence producer may be a provider platform, the evidence custodian may be Party IJK, and the evidence owner for assessment purposes may be Party ABC or Party EGH. Decision authority remains separate from technical execution.

The book also distinguishes readiness activities from official assessment activities. Gap assessments, readiness reviews, internal evidence validation, and mock interviews help an organization prepare. They do not themselves create an official CMMC Status. Formal status terminology should be used only in the context defined by the current CMMC program.

Terms such as compliant, certified, out of scope, FedRAMP equivalent, compensating control, and CMMC ready should be used with precision. A tool deployment, license purchase, cloud migration, or MSP contract does not independently establish the conclusion implied by those terms.

L.40 Authoritative Sources for This Glossary

- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program, including section 170.4 definitions.
- Department CMMC program About, Resources, Scoping, and Assessment Guide materials current at the publication verification date.
- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024).
- DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025).
- NIST SP 800-171 Revision 2 and the NIST publication-status record showing withdrawal on May 14, 2024 and supersession by Revision 3.
- NIST SP 800-171A June 2018 where referenced by the current CMMC Level 2 assessment methodology.
- NARA CUI Program materials and CUI Registry for authoritative CUI categories, authorities, and marking/handling context.

L.41 Final Closing Perspective

Appendix L is intended to remain beside the reader while the rest of the book is used. Its value is not the number of acronyms it contains, but the discipline it creates around language. When Party ABC, Party EGH, Party IJK, an assessor, a contracting professional, and a technician use the same term, they should understand the same responsibility, boundary, evidence expectation, or operational condition.

That common vocabulary supports the central theme of this book: CMMC readiness is strongest when contractual requirements, security architecture, managed-service operations, evidence, and organizational accountability describe the same real environment.

Appendix M

Operational Acceptance and Continuous Readiness Toolkit

Detailed Teaching and Operational Edition

M.1 Purpose of the Toolkit

The final appendix converts the concepts in this book into an operating system for the MSP and its defense-contractor customers. The objective is to prevent the familiar cycle in which an organization works intensely before an assessment, produces a temporary collection of screenshots and documents, and then allows the environment to drift after the assessment. Operational acceptance establishes a controlled entry point into normal service. Continuous readiness keeps the accepted environment supportable, evidenced, and explainable as people, technology, contracts, and threats change.

This toolkit is deliberately written for joint use. Party ABC or Party EGH remains responsible for organizational decisions and applicable contractual obligations. Party IJK can implement and operate substantial portions of the technical environment, produce recurring evidence, and identify drift. The toolkit makes those relationships visible instead of hiding them inside a general statement that the MSP handles security.

M.2 What Operational Acceptance Means

Operational acceptance is the formal internal decision that a system, service, customer environment, major change, migration, or remediation package is sufficiently understood and controlled to enter or return to normal operations. It is not a CMMC certification and does not replace an assessment.

A technically functional service is not necessarily operationally acceptable. A SIEM can ingest logs while lacking defined retention, alert ownership, escalation, evidence export, licensing, and offboarding procedures. A cloud migration can be technically complete while old data remains in an unintended repository. Operational acceptance catches these gaps before they become normal.

M.3 The Seven-Question Acceptance Model

Question	Acceptance Decision
Who owns it?	Organizational accountability.
Who decides?	Authority for access, exceptions, risk, outages, major changes, and return to service.
Who implements?	Team/provider that builds and configures.
Who operates?	Recurring administration, monitoring, review, maintenance, and response.
Who produces evidence?	System/process/person creating records.
Who maintains evidence?	Custody, retention, protection, indexing, retrieval.
Who independently assesses it?	Applicable self-assessment, C3PAO, DIBCAC, audit, or other review role.

M.4 Operational Acceptance Gate

The gate should occur before production onboarding, after a major migration or architecture change, after significant incident recovery, and before a remediated control is declared closed. The decision authority records acceptance, conditional internal acceptance with corrective actions, or rejection.

Gate Area	Minimum Evidence	Primary Owner
Scope/Architecture	Inventory, boundary/data-flow diagrams, connections, provider map	Customer + MSP
Identity/Privilege	Admin roles, MFA, least privilege, emergency access, service identities	Customer/IAM
Secure Configuration	Baselines, hardened configuration, change record, drift method	MSP
Logging/Monitoring	Sources, retention, alert routes, health, sample records	SOC/MSP
Vulnerability/Patching	Coverage, findings, remediation, exceptions	MSP + Risk Owner
Backup/Recovery	Protected design, restore evidence, retention	Service Owner
Incident Response	Contacts, escalation, alternate comms, preservation	Customer + MSP
Evidence	Mapping, location, freshness, retention, custodian	Evidence Owner
Documentation	SSP/procedure/runbook/diagram updates	Customer + MSP
Licensing/Support	Required features licensed;	Commercial Owner

	renewal/support ownership	
Offboarding	Export, revocation, disposition, evidence continuity	Customer + MSP

M.5 Acceptance Decision Record

Field	**Record**
Customer / Environment	_____
Service / Change	_____
Acceptance Scope	_____
Decision	Accepted / Conditionally Accepted / Rejected
Open Conditions	_____
Risk / Exception Approver	_____
Operational Owner	_____
Evidence Owner	_____
Acceptance Date	_____
Next Review / Trigger	_____

M.6 Continuous Readiness Operating Cycle

Continuous readiness observes the environment, compares it with the accepted state, investigates meaningful changes, corrects deficiencies, refreshes documentation and evidence, and escalates changes that may affect scope or compliance. Current DFARS 252.204-7021 makes continuing compliance particularly important because applicable contractors must maintain the required current CMMC status and complete annual affirmations of continuous compliance in SPRS for applicable CMMC UIDs.

Cadence	**Activity**	**Evidence**
Daily/Continuous	Security monitoring, backup jobs, tool health, identity/security alerts	SIEM/EDR/backup records
Weekly	Failed jobs, stale agents, critical vulnerabilities, privileged changes, unresolved incidents	Tickets/review
Monthly	Patch/vulnerability trends, lifecycle, exceptions, log coverage	Monthly packet
Quarterly	Scope, evidence sampling, access, restore,	Quarterly review

	drift, provider review	
Annually	SSP/policy, roles, incident exercise, supplier review, affirmation support	Annual package
Event-Driven	Major change, new CUI flow, migration, provider change, significant incident	Acceptance record

M.7 Daily and Weekly MSP Readiness Checklist

- Confirm critical security platforms are reporting and ticket monitoring gaps.
- Review failed backup, EDR, RMM, vulnerability, identity, and logging jobs.
- Escalate critical vulnerabilities under the customer's risk and emergency-change process.
- Review privileged changes and significant authentication/security alerts.
- Complete personnel access changes within defined timeframes.
- Ensure incidents and high-risk tickets have owners, next actions, and escalation dates.
- Preserve operational records in systems of record so evidence is created through normal work.

M.8 Monthly Security Operations Packet

Section	**Contents**
Environment Health	Coverage, platform health, outages, licensing
Identity	Joiners/movers/leavers, privileged changes, MFA exceptions
Vulnerability	Critical/high findings, aging, remediation, rescans
Patching	Coverage, failures, emergency patches, deferrals
Monitoring	Log coverage, SIEM/EDR health, significant alerts
Backup/Recovery	Job success, exceptions, restore validation
Incidents	Opened/closed incidents, lessons, corrective actions
Changes	Security-relevant production changes
Evidence	New artifacts, missing evidence, retention concerns
Decisions Needed	Risk, budget/license, architecture, approvals

M.9 Quarterly Continuous Readiness Review

The quarterly review is where operations and assessment readiness meet. It should challenge whether the documented environment still matches reality rather than merely present dashboards.

Question	Result
Has CUI/FCI flow changed?	Yes / No / Action
Are inventory and scope categories accurate?	Yes / No / Action
Are there new providers/cloud services?	Yes / No / Action
Have privileged roles/service identities changed?	Yes / No / Action
Are required security tools licensed, connected, reporting?	Yes / No / Action
Do SSP, diagrams, procedures and runbooks match operations?	Yes / No / Action
Can sampled evidence be retrieved and tied to requirements?	Yes / No / Action
Are remediation items aging?	Yes / No / Action
Have exceptions expired?	Yes / No / Action
Can personnel explain implementation consistently?	Yes / No / Action

M.10 Change-Triggered Readiness Review

Major changes should trigger readiness review rather than wait for the next calendar meeting. Examples include moving CUI, replacing identity providers, changing MSPs, adding subcontractors that receive CUI, changing cloud environments, replacing SIEM/EDR/RMM, acquisitions, new facilities, or recovery from a significant incident.

The change owner should determine whether scope, security requirements, SSP content, diagrams, responsibility assignments, evidence sources, licenses, incident procedures, or applicable CMMC records are affected.

M.11 Scope Change Intake Form

Field	Entry
Change Description	_____
Business / Technical Owner	_____
Effective Date	_____
New/Changed CUI or FCI Flow?	Yes / No — explain

New Asset/Service/Provider?	Yes / No — identify
Assessment Boundary Impact?	Yes / No / Unknown
SSP/Diagram Update?	Yes / No
Evidence Source Changed?	Yes / No
Incident/Logging Impact?	Yes / No
License/Contract Impact?	Yes / No
Acceptance Review Required?	Yes / No
Final Approver	_____

M.12 Evidence Health Toolkit

Evidence should be treated as an operational product. A mature environment knows where it originates, who can retrieve it, how long it remains available, and whether it still describes the current implementation.

Status	**Meaning**	**Action**
Current/Attributable	Identifies source, system and date/period	Retain/index
Current/Incomplete	Useful but does not fully support intended objective	Supplement
Stale	Earlier configuration/period	Refresh
Unattributed	Insufficient source/context	Recreate/export
Missing	No adequate artifact	Determine evidence vs implementation gap
Contradictory	Conflicts with documentation or another artifact	Investigate

M.13 Evidence Sampling Worksheet

Requirement/Topic	**Expected Evidence**	**Sample**	**Validated By**	**Result/Action**
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

M.14 Configuration and Tool-Health Review

Capability	**Health Question**	**Evidence**

EDR/MDR	Are expected endpoints enrolled, current, reporting?	Coverage + exceptions
SIEM	Are required sources ingesting and alerts functioning?	Source health + test
RMM	Are assets connected and privileged access controlled?	Agent/role report
Vulnerability	Is expected scope scanned and scanning healthy?	Coverage/history
Backup	Are jobs succeeding and representative restores valid?	History + restore
IAM	Are MFA, admin roles, policies, lifecycle operating?	Config + reviews
Cloud Security	Are required policies enabled under licensed tier?	Config + license

M.15 Exception and Risk Register

ID	**Exception/ Risk**	**Owner**	**Safeguard**	**Approval**	**Expiration**	**Status**
EX-___	_____	_____	_____	_____	_____	Open/Closed
EX-___	_____	_____	_____	_____	_____	Open/Closed

This is an internal governance tool. An internal exception does not waive a CMMC requirement or automatically create an authorized CMMC POA&M.

M.16 Remediation Closure Gate

Closure Test	**Question**
Root Cause	Was the underlying cause addressed?
Implementation	Was corrective action completed in production scope?
Validation	Was the result retested or independently checked?
Evidence	Is closure evidence current and attributable?
Documentation	Were SSP/procedure/diagram/baseline/runbook updated?
Recurrence	Is monitoring/process change in place?
Authority	Did the appropriate owner approve closure?

M.17 Incident-to-Readiness Feedback Loop

Incident Lesson	Readiness Update
Unknown asset/data flow	Inventory, diagrams, scope
Missing logs	Logging/retention/tool health
Excessive privilege	Roles, access review, IAM
Slow escalation	Contacts, severity, runbooks
Backup failure	Backup design and restore tests
Provider confusion	Responsibility matrix/SOW
Evidence unavailable	Retention, custody, export, index
Policy not followed	Training/process/monitoring

M.18 Annual Readiness and Affirmation Support Package

The annual review should provide the affirming official with disciplined, current information from which the organization can make its own required determination. The MSP supports that decision with accurate technical and operational evidence.

- Current system/asset inventory and scope categories.
- Current network and CUI/FCI data-flow diagrams.
- Current SSP and security procedures.
- Responsibility matrix covering customer and relevant providers.
- Access/privilege and personnel lifecycle evidence.
- Vulnerability, patching, configuration, logging, backup, and incident evidence.
- Open remediation and exception register.
- Provider/subcontractor review where relevant.
- Evidence-health sampling results.
- Material-change statement since the prior assessment/status date.
- Management review and issues requiring resolution before affirmation.

M.19 Multi-Customer MSP Dashboard

Customer	Scope Change	Critical Gaps	Evidence Health	Exceptions	Next Review	Owner
Party ABC	None/Open	___	Good/Watch/ Action	___	_____	_____
Party EGH	None/Open	___	Good/Watch/	___	_____	_____

			Action			
Customer ___	None/Open	___	Good/Watch/ Action	___	_____	_____

M.20 Customer Offboarding Readiness Gate

Offboarding is a security and evidence event. The parties should confirm access removal, credential/token revocation, data/evidence transfer or disposition, incident/finding handoff, license ownership, backup disposition, documentation transfer, and removal of provider automation.

Offboarding Item	**Complete**	**Evidence/Destination**
Privileged MSP access revoked	Yes/No	_____
RMM/EDR/provider agents handled	Yes/No	_____
API tokens/service principals handled	Yes/No	_____
Customer data/evidence exported	Yes/No	_____
Open incidents/findings handed off	Yes/No	_____
Backups handled per agreement	Yes/No	_____
Licenses transferred/terminated	Yes/No	_____
Final documentation delivered	Yes/No	_____
Customer transition accepted	Yes/No	_____

M.21 Party ABC Worked Example — New Customer Acceptance

Party ABC onboards Party IJK to operate identity, endpoints, SIEM monitoring, vulnerability management, and backup. ABC identifies the CUI environment and systems used for contract performance. IJK maps its services to that scope and identifies every privileged integration.

Before production acceptance, ABC approves administrative roles and emergency access. IJK verifies endpoint enrollment, log-source coverage, vulnerability scanning, backup jobs, restore capability, and evidence exports. The parties reconcile the SSP, network diagram, responsibility matrix, and runbooks with the actual configuration. Unresolved gaps receive owners and decision paths before ABC's authorized decision maker accepts the service.

M.22 Party EGH Worked Example — Major Cloud Migration

Party EGH moves a CUI workload to a different approved cloud architecture. The readiness trigger identifies consequences beyond file migration: CUI flow changes, old repositories must be retired, identity and logs change, backup locations change, and documentation must be updated.

The migration is not operationally complete merely because users can open files. Acceptance requires validation of access, cryptographic protection, monitoring, backup, privilege, evidence retention, prior-environment data disposition, documentation, and customer approval.

M.23 Party IJK Worked Example — MSP Platform Change

Party IJK replaces its RMM platform across multiple defense-contractor customers. Because the RMM is a privileged management plane, the change is treated as a security architecture event. IJK stages least-privilege roles, protects automation secrets, validates logging, removes the old platform, and verifies that abandoned agents or credentials do not remain.

Each customer receives its own acceptance record and evidence package because scope, licensing, endpoints, exceptions, and evidence ownership differ.

M.24 Continuous Readiness Calendar

Cadence	**Core Activity**
Monthly	Operations packet, gaps, evidence health, exception aging
Quarter 1	Scope/inventory + privileged access review
Quarter 2	Restore/recovery + incident tabletop
Quarter 3	Provider/license review + evidence sampling
Quarter 4	SSP/policy/readiness package + affirmation support
Major Change	Scope and operational acceptance review
Significant Incident	After-action remediation and re-acceptance as needed

M.25 Toolkit Governance

Party ABC or Party EGH should identify the organizational owner who approves the readiness process. Party IJK should identify the service lead responsible for recurring

operational inputs. Templates should be controlled, versioned, and tailored rather than completed once and forgotten.

The toolkit should evolve. Difficult evidence retrieval should improve the evidence process. Unclear incident authority should change the responsibility model. Cloud logging or licensing changes should update acceptance criteria. Continuous readiness is both a security process and a learning process.

M.26 Current Regulatory Caution

As of September 22, 2026, Department CMMC materials state that implementation is paused in Phase I. Current DFARS 252.204-7021 nevertheless establishes requirements, when the clause and required level apply, to have and maintain the required current CMMC status for applicable contractor information systems, complete annual affirmations of continuous compliance in SPRS for applicable CMMC UIDs, and close out a valid POA&M when operating under a Conditional CMMC Status. Organizations should verify current Department, 32 CFR part 170, DFARS, solicitation, and contract requirements before using this toolkit for a live procurement.

The toolkit is intentionally broader than the mechanics of an annual affirmation. Its purpose is to make continuing security claims supportable by ordinary operations, current evidence, defined responsibility, and controlled change.

M.27 Closing Perspective — From Assessment Project to Operating Discipline

The final lesson of this book is that certification preparation should mature into operational discipline. An organization that can pass an assessment only after months of emergency evidence collection has not achieved the strongest form of readiness. The more durable model is one in which security work creates evidence naturally, changes trigger scope and documentation review, incidents improve the environment, and ownership remains visible.

For Party ABC and Party EGH, organizational accountability remains active after an assessment. For Party IJK, managed services are designed not only to keep systems running but also to preserve the security state, evidence, and explainability customers need. Operational acceptance establishes the starting line. Continuous readiness keeps the organization there.

Used together with the preceding chapters and appendices, this toolkit closes the loop from readiness to assessment, from assessment to operations, and from operations back to continuing readiness.

M.28 Deepening Pass — 30/60/90-Day Continuous Readiness Launch

A customer that has just completed an assessment, migration, remediation project, or new MSP onboarding should not wait for the first annual review to discover that readiness has degraded. The first ninety days establish the operating rhythm. During the first thirty days, the parties stabilize ownership, evidence, monitoring, and open corrective actions. By sixty days, recurring evidence and exception management should be functioning. By ninety days, the customer should be able to conduct a representative readiness review without extraordinary preparation.

Period	Primary Objective	Required Outputs
Days 1–30	Stabilize accepted environment	Named owners; final inventory; evidence locations; tool-health baseline; open-action register
Days 31–60	Prove recurring operation	Monthly packet; access lifecycle evidence; vulnerability/patch cycle; backup/restore record; exception review
Days 61–90	Demonstrate sustainable readiness	Quarterly-style review; sampled evidence; staff interviews; change-trigger test; management decisions

M.29 Technician Shift and Service Checklist

Technicians are often the first people to see that a control is drifting. The toolkit therefore gives technicians a short operational lens that can be incorporated into ordinary service work without turning every ticket into a compliance project.

Technician Question	Action if No / Unknown
Is this asset/customer correctly identified?	Stop and validate customer, asset, and scope context.
Is the requested change authorized?	Obtain approval through the defined change/access process.
Will this affect CUI flow, security boundary, privilege, logging, or evidence?	Escalate for security/change-impact review.
Will the action disable or bypass a security control?	Use approved emergency/exception process.
Is the work recorded in the system of record?	Create/update the ticket before closure.
Is validation required after the change?	Perform and record test, rescan, health check, or peer review.
Does documentation need to change?	Assign/update the runbook, diagram, baseline, or SSP input.

Did the work create evidence that must be retained?	Export/link/index it according to customer procedure.

M.30 Control Owner Quarterly Attestation

The control-owner attestation is an internal management mechanism, not the formal CMMC annual affirmation. Its purpose is to force owners to review the implementation they are responsible for and disclose changes before the organization reaches the annual affirmation or next assessment.

Attestation Question	**Owner Response**
The documented implementation still reflects current operations.	Yes / No / Exception
Required recurring activities occurred during the quarter.	Yes / No / Exception
Material failures and exceptions are documented.	Yes / No / Exception
Evidence can be retrieved for the sampled period.	Yes / No / Exception
Provider responsibilities remain accurate.	Yes / No / Exception
No unreviewed scope-changing technology/service was introduced.	Yes / No / Exception
Open corrective actions have current owners and dates.	Yes / No / Exception
I have disclosed known material changes or gaps.	Yes / No / Details

M.31 MSP Service Acceptance Certificate

This certificate can be used when Party IJK places a new managed service into normal operation for Party ABC or Party EGH. It documents operational acceptance only; it is not a CMMC certificate and should never be presented as one.

Certificate Field	**Entry**
Customer	_____
Managed Service	_____
Production Scope	_____
Service Owner	_____
Customer Decision Authority	_____
Privileged Access Model Validated	Yes / No
Logging/Monitoring Validated	Yes / No

Backup/Recovery Dependency Validated	Yes / No / N/A
Evidence Export/Retention Validated	Yes / No
Runbook and Escalation Validated	Yes / No
Open Conditions	_____
Operational Acceptance Date	_____
Customer Approval	_____
MSP Service Lead	_____

M.32 Change-Impact Matrix

A disciplined change process distinguishes routine maintenance from changes that can alter assessment scope, evidence, or responsibility. The following matrix helps a service desk or change advisory process route higher-impact work correctly.

Change Type	Scope Review	Documentation	Evidence	Re-Acceptance
Routine approved patch	Usually No	Ticket/baseline as needed	Patch/validation record	No unless failure/material change
New endpoint handling CUI	Yes	Inventory/diagram/SSP input	Enrollment/ configuration	Yes
New cloud application	Yes	Data flow/provider/SSP	Configuration/logging	Yes
Identity provider change	Yes	Architecture/runbooks/ SSP	MFA/roles/logging tests	Yes
SIEM/EDR/RMM replacement	Yes	Provider/tool architecture	Coverage/retention/test	Yes
Firewall/routing redesign	Yes	Network diagram/baseline	Rule review/test	Yes
New subcontractor/ESP	Yes	Responsibility/provider records	Due diligence/agreement	Yes
Emergency containment	Evaluate	Incident/change record	Incident evidence	Post-incident review

M.33 Evidence Calendar

Evidence should be collected according to how the underlying activity occurs. A quarterly access review cannot be reconstructed credibly from a screenshot taken the day before an assessment. The evidence calendar ties collection to the operating cadence.

Evidence Area	Cadence	Producer	Custodian	Review

Security platform health	Daily/Weekly	MSP tools	MSP/customer repository	Monthly
Privileged access changes	Continuous	IAM/PSA	Customer/MSP	Monthly
Access review	Quarterly or policy cadence	Customer + MSP	Customer	Quarterly
Vulnerability scans	Defined recurring cadence	Scanner	MSP/customer	Monthly
Patch deployment	Monthly/emergency	RMM/endpoint tools	MSP	Monthly
Backup job records	Daily	Backup platform	MSP/customer	Monthly
Restore validation	Quarterly/defined cadence	Backup operator	Customer/MSP	Quarterly
Incident exercises	Annual/defined cadence	IR team	Customer	Annual
Scope/inventory validation	Quarterly + change-triggered	Customer/MSP	Customer	Quarterly
SSP/policy review	Annual + material change	Document owner	Customer	Annual

M.34 Management Readiness Review Package

Executives do not need raw telemetry from every tool. They need a decision package showing whether the environment remains supportable, where material risk is accumulating, and what decisions require organizational authority.

Management Section	**Decision Information**
Readiness Summary	Material changes, significant gaps, trend since prior review
Scope	New CUI flows, systems, providers, facilities, acquisitions
Risk	Critical vulnerabilities, aging remediation, exceptions
Operational Health	Security-tool coverage, logging, backup, identity
Incidents	Material events, lessons, unresolved corrective actions
Evidence	Sampling results and missing/stale evidence
Commercial Dependencies	Licensing, provider renewal, unsupported technology
Decisions	Risk acceptance, funding, staffing, architecture, contract questions
Next Milestones	Assessment/affirmation dates, major changes, exercises

M.35 Annual Readiness Package Index

The annual package should be assembled from records created throughout the year rather than built from scratch. The index below gives the organization a repeatable structure.

Tab	Package Content
1	Scope statement, inventory, diagrams, CUI/FCI flows
2	Current SSP and approved policies/procedures
3	Responsibility matrix and provider/service map
4	Identity, MFA, privileged access, lifecycle reviews
5	Configuration, change, vulnerability, and patch evidence
6	Logging, monitoring, SIEM/EDR, tool-health evidence
7	Backup, restore, media/data protection evidence
8	Incident response records, exercise, lessons learned
9	Training/personnel/physical evidence as applicable
10	Remediation, exception, risk, and closure records
11	Evidence sampling and internal readiness review
12	Management review and affirmation-support record

M.36 Operational Acceptance for a New External Service Provider

When a new ESP is introduced, the customer should not begin by asking only whether the provider has a security certification. The customer must understand what service is being consumed, what information or security function the provider touches, what administrative access exists, how the provider affects the assessment scope, what evidence the provider can supply, and how the relationship ends.

ESP Acceptance Topic	Required Determination
Service Function	What does the provider actually do?
Information Exposure	Does it process/store/transmit FCI/CUI or security protection data?
Administrative Reach	What privileged access or integrations exist?
Scope Impact	How does current CMMC scoping guidance treat the service?
Security Obligations	Which contract/security requirements apply?
Evidence	What artifacts can be supplied, how often, and in what format?

Incident Support	Notification, investigation, evidence, escalation responsibilities
Continuity	What happens during outage or provider failure?
Offboarding	Data export/disposition, credential revocation, evidence transfer

M.37 License and Feature Assurance Worksheet

Security designs often assume capabilities that exist only at a particular license tier. License assurance is therefore part of operational acceptance.

Platform / Feature	Required Tier	Current Tier	Owner	Renewal	Failure Impact
Identity / MFA / Conditional Access	_____	_____	_____	_____	_____
Audit / Log Retention	_____	_____	_____	_____	_____
Endpoint Security / EDR	_____	_____	_____	_____	_____
Email / Collaboration Security	_____	_____	_____	_____	_____
SIEM / Data Retention	_____	_____	_____	_____	_____
Backup / Immutable Retention	_____	_____	_____	_____	_____

M.38 Evidence Custody and Transfer Plan

An MSP may hold evidence that the customer needs years later. The parties should decide custody and transfer before an assessment or offboarding emergency.

Evidence Type	System of Record	Custodian	Retention	Customer Access	Exit Method
Tickets/changes	_____	_____	_____	_____	_____
Security alerts/incidents	_____	_____	_____	_____	_____
Audit logs	_____	_____	_____	_____	_____
Vulnerability reports	_____	_____	_____	_____	_____
Backup/restore	_____	_____	_____	_____	_____

records					
Configuration exports	_____	_____	_____	_____	_____

M.39 Continuous Readiness Metrics

Metrics should expose deterioration rather than reward superficial activity. Counting tickets closed or scans run can look positive while critical gaps age. The useful measures connect coverage, timeliness, exceptions, and evidence.

Metric	**Purpose**
Expected assets reporting to EDR/RMM	Detect coverage gaps
Required log sources healthy	Detect monitoring blind spots
Critical/high vulnerability aging	Expose remediation delay
Patch compliance with documented exceptions	Measure operational control
Privileged accounts reviewed	Detect access drift
Backup success plus restore-test success	Measure recoverability, not only job completion
Expired exceptions	Expose governance failure
Evidence samples passing validation	Measure assessment explainability
Open corrective actions past due	Expose readiness debt
Unreviewed scope-change events	Expose boundary/documentation drift

M.40 Readiness Escalation Thresholds

The organization should define which conditions require immediate management attention rather than waiting for the next scheduled review. Examples include discovery of an unapproved CUI repository, loss of a critical security log source, unsupported technology in the assessed environment, an expired security license that disables a required capability, an unreported material provider change, or evidence that a previously accepted control is no longer operating.

Escalation thresholds should identify the person who must be notified, the required response time, whether normal change controls may be accelerated, and whether the issue triggers a scope review, incident process, risk decision, or re-acceptance.

M.41 Complete Party ABC 90-Day Implementation Example

Day 1 begins with Party ABC and Party IJK confirming the accepted service boundary. ABC owns organizational policy, contract interpretation, risk decisions, and the decision to affirm continuous compliance. IJK owns the recurring managed operations defined in the service agreement. The parties identify the system of record for assets, tickets, identity changes, vulnerabilities, incidents, and evidence.

During the first month, IJK validates EDR/RMM coverage, required log sources, vulnerability scanning, backup health, privileged technician roles, and customer escalation contacts. ABC validates the current CUI flow, system inventory, provider list, and decision authorities. Any mismatch between the SSP and production is opened as a corrective action rather than quietly editing evidence to look consistent.

During days 31 through 60, the recurring operating cycle produces its first complete monthly packet. IJK demonstrates that failed jobs become tickets, critical vulnerabilities have owners, privileged changes can be traced to authorization, and backup records include a representative restore validation. ABC reviews exceptions and makes the decisions that only the customer can make.

During days 61 through 90, the parties conduct a representative quarterly readiness review. They select evidence from different weeks rather than the most convenient current screenshot. Personnel explain how access, vulnerability management, monitoring, backup, and incident escalation actually operate. A simulated scope change tests whether a new cloud service would be routed through the change-impact process. The result is not an artificial pre-assessment exercise; it is proof that ordinary operations are producing a defensible readiness state.

M.42 Party EGH — Readiness Recovery Scenario

Party EGH discovers that its documentation says all managed endpoints report to EDR, but a newly acquired group of laptops was never enrolled. This is both an implementation and evidence problem. The readiness process opens a material corrective action, determines whether CUI was present on the affected devices, evaluates incident implications, enrolls the devices, validates policy and logging, and updates the acquisition/onboarding process that allowed the gap.

The corrective action is not closed when the agent is installed. Closure requires coverage verification, root-cause correction, evidence retention, and confirmation that the inventory and SSP remain accurate. The example demonstrates why continuous

readiness is designed to discover and correct drift rather than conceal it until assessment preparation.

M.43 Party IJK — Multi-Customer Evidence Factory

Party IJK can improve efficiency by engineering evidence production into its service platform. Standard RMM reports, SIEM health exports, vulnerability summaries, access-change tickets, backup restore records, and incident templates can be generated consistently across customers while remaining logically and contractually separated.

Standardization does not mean every customer receives identical evidence. Each package must map to the customer's actual scope, services, responsibilities, retention requirements, and assessment needs. The 'factory' is the repeatable process for producing trustworthy artifacts, not a generic binder copied between customers.

M.44 Annual Affirmation Support — Responsibility Boundary

Current DFARS 252.204-7021 requires applicable contractors to complete and maintain a current annual affirmation of continuous compliance in SPRS for each applicable CMMC UID. The MSP's role is to provide accurate operational evidence and disclose known changes or deficiencies within its service boundary. The affirming official's role is an organizational role defined by the CMMC framework and should not be blurred with routine MSP administration.

The annual support package should therefore include a management statement of known material changes, open remediation, expired exceptions, unresolved scope questions, and provider changes. The objective is not to manufacture a positive answer. It is to ensure the authorized official has current information before making the organization's required affirmation.

M.45 Current 2026 Implementation Note

The Department's current CMMC materials state that Phase II requirements, originally scheduled for November 10, 2026, were suspended on July 13, 2026, while Phase I self-assessment requirements remain in place. The Department states that during the pause it will enforce NIST SP 800-171 Revision 2 compliance through self-assessments and select government-led assessments. This implementation posture should be rechecked before a live procurement or assessment because the Department has announced a comprehensive CMMC review.

The toolkit remains useful during that pause because its purpose is broader than preparing for one assessment event. It supports the underlying operational protection of FCI/CUI, accurate self-assessment, controlled change, evidence integrity, and readiness for future contractual or assessment requirements.

M.46 Deepening-Pass Closing Perspective

At this stage, Appendix M should be viewed as the operating companion to the entire book. The earlier chapters explain CMMC concepts, architecture, controls, evidence, assessment, and MSP responsibilities. This appendix turns those concepts into recurring actions, decision records, worksheets, review packages, and escalation triggers.

The next substantive pass should deepen the toolkit still further around governance charters, role-specific checklists, assessment-year planning, provider transition, incident re-acceptance, evidence retention, and complete reusable master templates. The final pass can then verify regulatory language, normalize the templates, and freeze the appendix as the book's operational close.

M.47 Substantive Expansion — Continuous Readiness Governance Charter

A continuous readiness program needs a charter so that readiness is not treated as an informal favor performed by the security team. The charter establishes purpose, authority, scope, recurring forums, escalation, records, and the relationship between the customer and its providers. It should be approved by an executive or other organizational authority capable of resolving cross-functional disputes.

Charter Element	Required Definition
Purpose	Maintain operational security, evidence, scope accuracy, and assessment explainability.
Executive Sponsor	Person with authority to resolve organizational barriers and resource decisions.
Program Owner	Person accountable for the readiness operating cycle.
Technical Operations	MSP/internal teams responsible for recurring implementation and monitoring.
Scope Authority	Person/team approving system boundary and CUI/FCI flow determinations.
Risk Authority	Person authorized to accept or escalate organizational risk.
Evidence Governance	Owner of evidence standards, repository, retention, and sampling.

Change Integration	How security/readiness review enters the change-management process.
Incident Integration	How incidents trigger corrective action, documentation review, and re-acceptance.
Meeting Cadence	Monthly operations; quarterly readiness; annual management review.
Escalation	Conditions requiring management, legal/contract, or incident escalation.
Records	Where decisions, attestations, exceptions, and acceptance records are retained.

M.48 Role-Specific Checklist — Executive Sponsor

The executive sponsor should not be expected to configure security tools. The sponsor's responsibility is to make sure unresolved security and readiness issues receive organizational decisions instead of remaining permanently in technical queues.

Executive Review	**Decision**
Material scope changes identified?	Acknowledge / Assign / Escalate
Critical remediation past due?	Fund / Prioritize / Risk decision
Unsupported or end-of-life systems?	Replace / Isolate / Approved plan
Security license or provider gaps?	Approve commercial action
Expired exceptions?	Close / Renew with justification / Reject
Material incident corrective actions?	Approve ownership and deadlines
Assessment/affirmation milestone approaching?	Confirm management readiness review
Known statement/documentation inconsistency?	Require correction before formal representation

M.49 Role-Specific Checklist — Customer Security or Compliance Lead

Responsibility	**Recurring Action**
Scope	Reconcile inventory, diagrams, CUI flow, providers, facilities.
SSP	Ensure documented implementation reflects production.
Responsibility	Maintain customer/MSP/ESP/CSP responsibility mapping.

Evidence	Sample artifacts and resolve missing/contradictory records.
Remediation	Track gaps, POA&M-eligible items where applicable, and internal corrective actions.
Exceptions	Review justification, approval, safeguards, expiration.
Assessment Readiness	Coordinate interviews, evidence, demonstrations, and assessor logistics.
Affirmation Support	Prepare current facts and unresolved issues for the authorized affirming official.

M.50 Role-Specific Checklist — MSP Service Manager

Responsibility	**Recurring Action**
Service Boundary	Confirm services and customer responsibilities remain understood.
Operational Health	Review RMM, EDR, SIEM, backup, vulnerability and IAM service health.
Escalation	Ensure material failures and scope changes reach the customer owner.
Evidence Production	Confirm recurring reports/tickets/exports are generated and retained.
Technician Access	Review privileged MSP access and personnel changes.
Change Control	Route security-relevant changes through required approval and validation.
Incidents	Ensure technical facts, evidence, chronology and customer communications are preserved.
Offboarding	Maintain a tested method to transfer evidence and revoke provider access.

M.51 Role-Specific Checklist — Technician

The technician checklist is designed to prevent a well-intentioned troubleshooting action from silently changing the assessed environment.

Before Work	**During Work**	**Before Closure**
Confirm customer, asset, authorization and ticket.	Use approved admin identity and procedure; record deviations.	Validate result and security-tool health.
Check whether work touches CUI path or security boundary.	Preserve required logs/evidence.	Attach/export evidence to system of record.
Check whether security control will be disabled/bypassed.	Escalate unexpected scope/security condition.	Update documentation task if architecture/config changed.

Confirm rollback/emergency plan where needed.	Do not make unauthorized risk decisions.	Record who approved and what was tested.

M.52 Role-Specific Checklist — Evidence Custodian

Control	Custodian Action
Repository	Maintain controlled storage with appropriate access.
Naming/Index	Use consistent customer, requirement/topic, source, and date identifiers.
Attribution	Preserve source system, export context, and operating period.
Retention	Apply documented retention and prevent premature deletion.
Integrity	Protect records from unauthorized modification.
Retrieval	Test that evidence can be located without relying on one employee.
Transfer	Maintain export/offboarding method for provider-held evidence.
Sensitive Content	Avoid unnecessary replication of CUI or secrets in evidence repositories.

M.53 Assessment-Year Planning Calendar

A three-year assessment cycle should not become two quiet years followed by one year of panic. The operating model below treats every year as a readiness year while increasing formal preparation as the next required assessment approaches.

Period	Readiness Focus
Post-Assessment Months 1–3	Close lessons learned, stabilize accepted environment, validate evidence ownership.
Months 4–12	Operate monthly/quarterly cycle; correct drift; complete annual review/affirmation support.
Year 2	Repeat evidence sampling; test personnel depth; review providers; validate major changes.
Year 3 Early	Reconfirm scope and assessment path; identify stale documents and evidence weaknesses.
Year 3 Mid	Run full readiness review across requirements and assessment objectives; remediate.
Pre-Assessment	Freeze logistics, validate evidence index, interviews, safe demonstrations, assessor access.
Assessment Period	Maintain normal operations; control changes; respond with

	attributable evidence.
Immediately After	Capture lessons, corrective actions, evidence retention, and new acceptance baseline.

M.54 Incident Re-Acceptance Package

A significant incident can invalidate assumptions that supported the prior acceptance decision. Re-acceptance determines whether the recovered environment is safe and sufficiently understood to resume normal operations.

Re-Acceptance Element	**Evidence / Decision**
Incident Scope	Affected systems, identities, data, providers and time period.
Containment Complete	Evidence that active threat pathways are controlled.
Eradication	Persistence, malicious artifacts, compromised credentials, vulnerabilities addressed.
Recovery Validation	Systems restored from trusted state and required services tested.
Credential Reset	Affected user/admin/service secrets rotated as required.
Security Tool Health	Logging, EDR, SIEM, vulnerability and backup functions validated.
Architecture Change	Emergency segmentation/configuration reflected in diagrams/baselines.
Evidence Preservation	Incident and forensic records protected and retained.
Corrective Actions	Root-cause actions assigned with owners and dates.
Return-to-Service Authority	Named person approves production return.
Post-Incident Monitoring	Heightened monitoring period and exit criteria defined.

M.55 Provider Transition Package

Changing MSPs can create one of the largest temporary security gaps in a managed environment. Both outgoing and incoming providers may hold privileged access, automation, documentation, evidence, and institutional knowledge. Transition should therefore be managed as a controlled security project.

Transition Domain	**Outgoing Provider**	**Incoming Provider**	**Customer**
Privileged Access	Inventory/export/revoke at handoff	Create least-privilege access	Approve and validate
RMM/Agents	Remove or transfer as agreed	Deploy/validate new tooling	Confirm coverage

Secrets/API	Identify and revoke/rotate	Create new controlled secrets	Own approvals
Evidence	Export agreed historical records	Import/index where needed	Verify receipt/retention
Open Incidents	Provide chronology/status	Accept operational handoff	Approve ownership
Open Vulnerabilities	Provide findings/exceptions	Validate and continue remediation	Set priorities
Documentation	Transfer current runbooks/configs	Validate against production	Accept discrepancies/actions
Backups	Transfer/retain/dispose per agreement	Validate new service	Approve retention/disposition
Licenses	Identify ownership/end dates	Establish new entitlements	Approve commercial transition

M.56 Evidence Retention Matrix

Retention should be based on contractual obligations, assessment needs, incident requirements, legal/business needs, and the useful operating period of the evidence. The matrix below is intentionally a planning template rather than a universal retention schedule.

Evidence Class	**Example**	**Owner**	**Minimum/ Required Retention**	**System**	**Disposition**
Assessment	Evidence index, assessor requests	_____	Per applicable requirement/policy	_____	_____
Identity	Access reviews, admin changes	_____	_____	_____	_____
Audit/Logs	Security/audit events	_____	_____	_____	_____
Vulnerability	Scans, rescans, exceptions	_____	_____	_____	_____
Change	Approvals, validation	_____	_____	_____	_____
Backup	Job/restore evidence	_____	_____	_____	_____
Incident	Chronology, reports, images	_____	Applicable contract + policy	_____	_____
Training	Completion/role training	_____	_____	_____	_____
Provider	Due diligence, agreements	_____	_____	_____	_____

M.57 Management Sign-Off Package

Management sign-off should be a decision process, not a signature page placed in front of unresolved facts. The package should make material issues difficult to overlook.

Management Statement	Status
Scope has been reviewed for material changes.	Confirmed / Exception
Known critical implementation gaps are disclosed.	Confirmed / Exception
Open remediation and exceptions are current.	Confirmed / Exception
Required security services are licensed and operating.	Confirmed / Exception
Provider responsibilities and dependencies are current.	Confirmed / Exception
Evidence sampling identified no undisclosed material contradiction.	Confirmed / Exception
Significant incidents and corrective actions are disclosed.	Confirmed / Exception
Decisions requiring management authority are resolved or explicitly recorded.	Confirmed / Exception

M.58 Master Continuous Readiness Register

The master register gives the program owner one place to see issues that cross tool and departmental boundaries. It should link to detailed tickets rather than duplicate every technical field.

ID	Type	Customer/ System	Issue/ Change	Owner	Due	Risk	Evidence	Status
CR-___	Gap/ Change/ Exception	_____	_____ _____	_____	_____	_____	_____	_____
CR-___	Gap/ Change/ Exception	_____	_____ _____	_____	_____	_____	_____	_____
CR-___	Gap/ Change/ Exception	_____	_____ _____	_____	_____	_____	_____	_____

M.59 Master Operational Acceptance Worksheet

Acceptance Domain	Validated By	Evidence Reference	Open Condition	Decision
Scope and Data Flow	_____	_____	_____	Pass/Condition/Fail
Identity and Privilege	_____	_____	_____	Pass/Condition/Fail
Configuration	_____	_____	_____	Pass/Condition/Fail
Logging/Monitoring	_____	_____	_____	Pass/Condition/Fail
Vulnerability/Patching	_____	_____	_____	Pass/Condition/Fail
Backup/Recovery	_____	_____	_____	Pass/Condition/Fail
Incident Readiness	_____	_____	_____	Pass/Condition/Fail
Evidence/Retention	_____	_____	_____	Pass/Condition/Fail
Documentation	_____	_____	_____	Pass/Condition/Fail
Providers/Licensing	_____	_____	_____	Pass/Condition/Fail
Offboarding/Continuity	_____	_____	_____	Pass/Condition/Fail

M.60 Evidence Request Tracker

Request ID	Requirement/ Topic	Requested Artifact	Source/ Owner	Due	Delivered	Validation
ER-___	_____	_____	_____	_____	_____	_____
ER-___	_____	_____	_____	_____	_____	_____
ER-___	_____	_____	_____	_____	_____	_____

The tracker is useful during internal sampling and formal assessment preparation. It exposes evidence that depends on a single technician, provider portal, expiring license, or manual reconstruction.

M.61 Interview Readiness Worksheet

Role	Topics to Explain	Evidence/Systems Used	Backup Interviewee	Gap/Action
System Owner	Scope, business use, responsibility	_____	_____	_____
IAM Administrator	Account lifecycle, MFA,	_____	_____	_____

	privilege			
SOC Analyst	Monitoring, triage, escalation	_____	_____	_____
MSP Technician	Change, patch, configuration	_____	_____	_____
Incident Lead	Response, reporting support, preservation	_____	_____	_____
Evidence/Compliance Lead	SSP, evidence, remediation	_____	_____	_____

Interview preparation should improve understanding, not teach personnel to recite scripted answers. If two people describe the same process differently, the program should determine whether the problem is training, documentation, responsibility, or actual implementation.

M.62 Safe Demonstration Plan

Demonstration	**Production Risk**	**Test Method**	**Expected Result**	**Fallback**
MFA/Access Control	Low/Med	Approved test account	Policy enforced	Screens/export
Account Disablement	Med	Test identity	Access removed	Audit evidence
Logging	Low	Generate benign event	Event visible/correlated	Historical sample
EDR	Med	Vendor-approved benign test	Detection/escalation	Prior test record
Backup Restore	Med	Controlled representative restore	Data restored/validated	Prior restore record
Boundary Rule	Med/High	Approved test path	Unauthorized path denied	Config + prior test

No assessment demonstration should introduce unnecessary production risk. The organization should know which demonstrations are safe, which require maintenance windows or test systems, and which are better supported through existing evidence and assessor-approved methods.

M.63 Substantive Party ABC End-to-End Case Study — Starting Condition

Party ABC is a small defense contractor with approximately one hundred employees. It handles CUI for engineering and program-management work. Party IJK provides

managed Microsoft administration, endpoint management, EDR, SIEM, vulnerability management, backup, and help desk. A specialized cloud provider supports one engineering application. ABC has completed a major readiness project, but management wants the environment to remain ready without repeating that project every year.

The first governance decision is to make ABC the owner of organizational policy, scope decisions, contract interpretation, risk acceptance, and formal representations. IJK is the operator for defined managed services and an evidence producer for those services. The engineering cloud provider owns and operates portions of its service under the applicable agreement. The parties document these relationships instead of relying on the phrase 'fully managed IT.'

M.64 Party ABC Case Study — Operational Acceptance

ABC and IJK conduct the master operational acceptance worksheet. The inventory is compared with EDR, RMM, vulnerability, identity, and network records. Two stale laptops remain in inventory but have been disposed of; their disposition records are attached and inventory is corrected. One engineering workstation is active but missing from vulnerability scanning. It is not accepted as complete until scanning coverage is restored and validated.

The identity review finds that IJK has five technician accounts with standing global administrative privileges even though only two roles require that level of access. IJK redesigns its role assignments and emergency process. ABC approves the new model. The acceptance package retains the before-and-after authorization and configuration evidence.

M.65 Party ABC Case Study — First Monthly Cycle

During the first month, the SIEM health review shows that a firewall log source stopped sending events after a firmware update. The MSP does not wait for quarterly review. A ticket is opened, ingestion is restored, and the service manager records the monitoring gap period. The event demonstrates the value of monitoring the monitoring system itself.

The monthly vulnerability review also identifies a critical finding on a server supporting CUI. ABC's change window would normally delay remediation. The predefined escalation threshold routes the issue to the authorized risk and change

decision makers. The resulting emergency change is documented, tested, rescanned, and closed with evidence.

M.66 Party ABC Case Study — Quarter-End Readiness Review

At quarter end, ABC samples evidence rather than reviewing only dashboards. The team selects one terminated employee, one new privileged account, one critical vulnerability, one firewall change, one backup restore, and one security alert. Each sample must connect authorization, implementation, validation, and retained evidence.

The terminated employee sample reveals that Microsoft access was removed promptly but an external engineering application account remained active for six days. The issue becomes a corrective action affecting the offboarding process and provider responsibility map. This is exactly the type of cross-provider weakness that a dashboard limited to Microsoft's tenant would not reveal.

M.67 Party ABC Case Study — Material Change

Six months later, engineering proposes a new cloud collaboration platform. The procurement request triggers the change-impact matrix before the service is purchased. ABC determines whether CUI will be placed in the platform, what contractual and cloud-security conditions apply, how identities are managed, what logs are available, how data is exported, and how the provider affects scope.

Because the proposed service changes the CUI flow, the SSP, data-flow diagram, provider inventory, evidence plan, incident contacts, and offboarding plan are updated before production use. Operational acceptance becomes the final gate after technical deployment.

M.68 Party ABC Case Study — Incident and Re-Acceptance

Later in the year, an administrator's credentials are suspected of compromise. IJK's SOC performs triage and immediately escalates to ABC under the incident plan. The parties preserve logs and chronology, contain the identity, rotate relevant secrets, investigate administrative activity, and evaluate the applicable reporting obligations using the controlling contract language.

After recovery, ABC does not simply reopen access. The incident re-acceptance package validates identities, privileged roles, logging, EDR, relevant configurations,

and corrective actions. The incident reveals that one automation token had broader privilege than documented. The token is replaced with a narrower role, the responsibility record is corrected, and a recurring secret review is added.

M.69 Party ABC Case Study — Annual Management Review

At the annual review, management receives a package assembled from the year's normal operations: scope changes, evidence samples, vulnerabilities, patching, access reviews, incidents, restore tests, provider changes, exceptions, remediation, and security-tool health. The package identifies unresolved issues rather than hiding them.

The authorized organizational official can then make the required decisions using current information. Party IJK supplies its operational evidence and disclosure of known service-boundary issues, but ABC retains its organizational accountability. The annual review therefore becomes the culmination of a year's operating discipline rather than a last-minute evidence hunt.

M.70 Party ABC Case Study — Lessons for the MSP

For Party IJK, the ABC program demonstrates that continuous readiness can be standardized without becoming generic. IJK uses the same acceptance framework, evidence-health model, monthly packet, and transition process across customers. The customer-specific elements—scope, contracts, providers, licensing, responsibilities, evidence retention, and decision authority—remain separately documented.

This approach also creates a stronger managed service. Coverage gaps are discovered faster, customer decisions are documented, provider transitions are safer, and evidence is available for troubleshooting and incident response as well as assessment. CMMC readiness becomes an operational-quality discipline rather than a separate compliance workload.

M.71 Master Toolkit Index

Toolkit Item	**Primary Use**
Seven-Question Acceptance Model	Clarify accountability and operational roles
Operational Acceptance Gate	Authorize production operation
Acceptance Decision Record	Document decision and conditions
30/60/90-Day Launch	Stabilize post-project/post-assessment operations
Technician Checklist	Control day-to-day changes

Control Owner Attestation	Quarterly internal accountability
MSP Service Acceptance Certificate	Accept managed service into operation
Change-Impact Matrix	Identify scope/evidence/documentation impacts
Evidence Calendar	Create evidence through normal operations
Management Readiness Package	Support executive decisions
Annual Readiness Package	Prepare affirmation/assessment evidence
ESP Acceptance Worksheet	Govern external providers
License Assurance Worksheet	Prevent capability loss from licensing
Evidence Custody Plan	Protect access/retention/transfer
Readiness Metrics	Detect deterioration
Incident Re-Acceptance Package	Return safely after significant incident
Provider Transition Package	Change MSP/ESP without security gaps
Evidence Retention Matrix	Plan retention and disposition
Master Readiness Register	Track cross-functional readiness issues
Evidence Request Tracker	Control sampling/assessment requests
Interview Worksheet	Prepare knowledgeable personnel
Safe Demonstration Plan	Test without unnecessary production risk

M.72 Substantive Expansion Closing Perspective

Appendix M now serves as the operational handoff for the book. A reader can move from understanding CMMC to assigning responsibility, accepting services, operating controls, producing evidence, detecting drift, governing providers, responding to incidents, transitioning MSPs, supporting annual management decisions, and preparing for the next assessment without rebuilding the program from zero.

The final pass should now focus on editorial consistency, authoritative regulatory verification, template normalization, page-layout quality, and publication readiness. The substance of the toolkit is intentionally broad because continuous readiness is not one checklist; it is the integration of governance, technical operations, evidence, change, incident response, provider management, and organizational decision authority.

M.73 Final Regulatory Verification and Publication Note

This toolkit is an operational teaching resource. It does not replace 32 CFR part 170, the applicable FAR or DFARS clauses, a solicitation or contract, current CMMC program guidance, or authoritative NIST publications. Before using a template for a live procurement, assessment, affirmation, incident, or contractual decision, the organization should verify the current controlling requirements.

Final verification on September 22, 2026 confirms that current Department CMMC materials state that Phase II requirements, originally scheduled for November 10, 2026, were suspended on July 13, 2026, while Phase I self-assessment requirements remain in place. The Department states that during the pause it will enforce NIST SP 800-171 Revision 2 compliance through self-assessments and selected government-led assessments. Because the Department has announced a comprehensive CMMC review, readers should recheck implementation status before relying on a future milestone.

Current DFARS 252.204-7021 (NOV 2025) requires, when the clause and specified CMMC level apply, that the contractor have and maintain a current CMMC status for applicable contractor information systems used to process, store, or transmit FCI or CUI. The clause also requires annual affirmation of continuous compliance in SPRS for each applicable CMMC UID, addresses flowdown, and requires successful closeout of a valid POA&M when the contractor holds a Conditional CMMC Status.

The same clause defines current Conditional Level 2 status as not older than 180 days, subject to the applicable conditions, and current Final Level 2 status as not older than three years, with a corresponding affirmation of continuous compliance not older than one year. These formal program terms should remain distinct from the internal operational-acceptance and readiness records in this appendix.

NIST SP 800-171 Revision 2 was withdrawn by NIST on May 14, 2024 and superseded by Revision 3. Current CMMC implementation materials nevertheless continue to reference Revision 2 for the Level 2 baseline during the present implementation posture. This appendix therefore distinguishes the current NIST publication from the baseline identified by current CMMC program materials.

M.74 Final Use Standard for the Toolkit

The worksheets in Appendix M should be tailored, not mechanically completed. A blank field is not evidence, a signature does not correct an implementation gap, and

an internal exception does not waive a contractual or CMMC requirement. Each organization should connect the toolkit to its real systems of record, actual service agreements, current scope, decision authorities, evidence sources, and operating cadence.

Party ABC and Party EGH should retain organizational authority for contractual interpretation, scope decisions, risk acceptance, formal representations, and affirmations. Party IJK can implement and operate managed capabilities, produce evidence, identify drift, and support management decisions. Where an independent assessment is required, readiness support and managed operations remain distinct from the independent assessment role.

M.75 Authoritative Sources for Final Verification

- Current Department CMMC About and Resources materials, including the July 13, 2026 Phase II suspension notice and Phase I implementation posture.
- 32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program.
- DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025).
- DFARS subpart 204.75, Cybersecurity Maturity Model Certification.
- NIST SP 800-171 Revision 2 publication-status record and NIST SP 800-171 Revision 3 (May 2024).
- Applicable solicitation, contract, task order, delivery order, and flowdown language for each live customer engagement.

M.76 Final Closing Perspective

Appendix M closes the book by moving CMMC from a preparation project into an operating discipline. Operational acceptance establishes a defensible starting state. Continuous readiness preserves that state through ordinary work: controlled change, healthy security tools, current scope, recurring evidence, provider governance, incident learning, remediation, and management decisions.

For the MSP, the central lesson is that technical service delivery and assessment readiness should reinforce one another. The same ticket that authorizes a privileged change can become evidence. The same tool-health review that detects a failed agent can prevent an assessment gap. The same incident review that improves containment can correct documentation and responsibility. When those processes are designed together, readiness becomes sustainable rather than episodic.

For the defense contractor, the central lesson is that outsourcing operations does not eliminate organizational accountability. The strongest model is a documented partnership in which each party knows what it owns, what it decides, what it implements, what it operates, what evidence it produces and maintains, and who independently assesses the result when an assessment is required.

With that operating model in place, the journey described throughout this book reaches its intended destination: not merely readiness for one CMMC event, but a repeatable program capable of protecting information, supporting contractual obligations, producing trustworthy evidence, and adapting as technology and requirements change.