The CMMC Compliance Playbook

(2025 Edition)

Provided by:

CAPE ENDEAVORS

CAPE ENDEAVORS

Table of Contents

INTRODUCTION

Cybersecurity threats are increasing in scale, sophistication, and impact—especially within the defense industrial base (DIB). As a result, the U.S. Department of Defense (DoD) established the Cybersecurity Maturity Model Certification (CMMC) program to ensure contractors implement adequate cybersecurity practices to protect Controlled Unclassified Information (CUI). This guide is designed for defense contractors seeking practical advice, industry-aligned strategies, and compliance tools to navigate the 2025 landscape of CMMC 2.0.

CMMC 2.0 Overview & Timeline

The CMMC 2.0 framework simplifies the original five-tier model into three levels, aligning more closely with existing federal cybersecurity standards like FAR 52.204-21 and NIST SP 800-171. It aims to ensure defense contractors implement appropriate safeguards to protect Federal Contract Information (FCI) and CUI.

CMMC 2.0 replaces the original five-level model with a simplified three-level framework:

Level 1: Foundational

- **Scope:** Applies to contractors that process, store, or transmit FCI. FCI is defined in 48 CFR § 4.1901 and includes information not intended for public release that is provided by or generated for the government under a contract.
- **Requirements:** Implements the 15 basic safeguarding requirements outlined in FAR 52.204-21 (b)(1)(i)–(xv). These are interpreted by the DoD as 17 distinct practices within the CMMC framework, as detailed in the Cybersecurity Maturity Model Certification (CMMC) Model Overview v2.13 (p. 12–48).
- **Practices:** Organizations must implement 17 cybersecurity practices that represent essential protections for information systems handling FCI. These practices are mapped to and derived from FAR 52.204-21 but are expressed in a more granular format for assessment purposes.
- **Assessment:** Requires an annual self-assessment, performed in accordance with 32 CFR § 170.15, and an executive-level affirmation submitted through the Supplier Performance Risk System (SPRS).
- **Domains Covered** (6 total/17 practices):
  - Access Control (AC) – 4 practices
  - Identification and Authentication (IA) – 2 practices
  - Media Protection (MP) – 1 practice
  - Physical Protection (PE) – 2 practices
  - System and Communications Protection (SC) – 2 practices
  - System and Information Integrity (SI) – 6 practices
- **Purpose:** These 17 practices represent foundational cyber hygiene requirements designed to protect FCI from unauthorized access, use, or disclosure. They provide a baseline level of security for all DoD contractors, regardless of size or contract scope.

CMMC 2.0 Overview & Timeline

Level 2: Advanced

- **Scope:** Applies to contractors and subcontractors that process, store, or transmit CUI in support of DoD contracts.
- **Requirements**: Implements the 110 security requirements outlined in **NIST SP 800-171 Revision 3**, which provides the framework for protecting CUI in nonfederal systems. The **CUI Overlay Spreadsheet** provides a detailed mapping of the 110 requirements to their corresponding NIST SP 800-53 controls, including organization-defined parameters (ODPs) and tailoring decisions.
- **Assessment Requirements:**
  - Triennial third-party assessments are required for prioritized acquisitions, conducted by a **certified CMMC Third-Party Assessor Organization (C3PAO)**.
  - For non-prioritized acquisitions, annual self-assessments are permitted (per **32 CFR § 170.16**, pending final rule adoption).
  - Contractors may be issued a conditional certification if:
    - Their CMMC score is ≥88,
    - All "high-weight" 5-point controls are implemented, and
    - Remaining deficiencies are documented in a Plan of Action and Milestones (POA&M).
  - Under conditional certification, organizations have up to 180 days to remediate the POA&M items (see **32 CFR § 170.24**).
- **Domains Covered:**
  - The 110 controls are mapped across 14 domains, aligned with the security requirement families in NIST SP 800-171:

    - Access Control (AC)
    - Awareness & Training (AT)
    - Audit & Accountability (AU)
    - Configuration Management (CM)
    - Identification & Authentication (IA)
    - Incident Response (IR)
    - Maintenance (MA)
    - Media Protection (MP)
    - Personnel Security (PS)
    - Physical Protection (PE)
    - Risk Assessment (RA)
    - Security Assessment (CA)
    - System & Communications Protection (SC)
    - System & Information Integrity (SI)

- **Objective:** Level 2 is designed to safeguard CUI against advanced persistent threats (APTs) and ensure compliance with Defense Federal Acquisition Regulation Supplement **(DFARS) Clause 252.204-7012**, which mandates NIST 800-171 implementation.

CMMC 2.0 Overview & Timeline

Level 3: Expert

- **Scope:** Level 3 is intended for defense contractors that handle highly sensitive CUI requiring strong protection against APTs. It applies to contracts critical to national security and key DoD programs, and it ensures that the contractor—referred to as the Organization Seeking Certification (OSC)—can safeguard CUI at a level appropriate to the risk. This includes protecting how CUI is shared with the government and across multi-tiered supply chains involving subcontractors.
- **Requirements**: The specific requirements may undergo additional revisions and roll-out is not anticipated until Q3/2026. But the current **CMMC Assessment Guide Level 3 Assessment Guide Version 2.13**, published September of 2024 is available for review.

CMMC Rollout Timeline

2025
Spring/Summer 2025 CMMC Final Rule published.

2025
Late 2025: DoD begins phased implementation.

2026/27
CMMC requirements become mandatory in select RFPs.

Risks of Non-Compliance

Failure to comply with CMMC requirements poses significant risks:

Contract Termination or Ineligibility

Contractors must hold a valid CMMC certification at the required level at the time of award:

- Level 1: Annual self-assessment
- Levels 2: Assessment by a certified C3PAO

Per **DFARS 252.204-7021**, certification is mandatory for both primes and subcontractors and must be maintained throughout the contract.
Additionally, contractors must submit their NIST SP 800-171 scores to the SPRS per **DFARS 252.204-7019/7020**. Contracting officers review these scores during supplier selection.

Bottom Line: No certification = no eligibility to bid, win, or keep DoD contracts.

False Claims Act Liability and Cybersecurity Misrepresentation

Contractors that falsely claim adherence to NIST SP 800-171 or CMMC may face whistleblower actions, False Claims Act (FCA) penalties, and reputational damage.

- In March 2025, **MORSECORP Inc. paid $4.6M** to settle allegations of falsely claiming compliance despite failing to implement required controls and submitting inaccurate SPRS scores.
- In May 2025, **Raytheon Companies and Nightwing Group agreed to pay $8.4M** for similar FCA violations tied to non-compliance with federal cybersecurity requirements.

Bottom Line: Misrepresenting your compliance—even accidentally—can cost millions in False Claims Act penalties and trigger whistleblower lawsuits.

Contact Us 888-951-7675 www.capeendeavors.com info@capeendeavors.com

Risks of Non-Compliance

Affirmation and Criminal Liability –

Under the final CMMC rule, each Organization Seeking Certification (OSC) must designate a senior-level representative—called the affirming official—to attest to the accuracy of their self-assessment or third-party certification.

This affirmation is a legally binding declaration, not a formality. False statements may trigger criminal prosecution under **18 U.S. Code § 1001** and False Claims Act liability. SPRS now requires individual attestation for each of the 110 NIST 800-171 controls, meaning each error could be treated as a separate false claim.

Bottom Line: The affirming official is personally accountable—false attestation can lead to **criminal charges** under federal law.

Reputational Damage –

Failing a C3PAO assessment or appearing noncompliant in the SPRS can severely damage a contractor's reputation and limit future DoD opportunities.

The SPRS is the DoD's official platform for assessing contractor risk, including cybersecurity posture. Contracting officers and prime contractors use SPRS data during source selection and subcontractor evaluation.

Bottom Line: Appearing as noncompliant in the SPRS or failing a C3PAO audit can harm a company's standing, limiting future DoD opportunities.

Mapping NIST 800-171 to Real-World Implementation

CAPE ENDEAVORS

NIST SP 800-171 includes 110 cybersecurity requirements grouped into 14 categories (called “control families”). Below are examples of how companies commonly meet those requirements using real tools and technologies.

Control Family	Example Technologies/Implementations
Access Control (AC)	Role-based access control (RBAC), multi-factor authentication (MFA), identity and access management (IAM) solutions (e.g., Okta, Azure AD), single sign-on (SSO), privileged access management (PAM) tools (e.g., CyberArk).
Awareness & Training (AT)	Role-Based Risk Awareness, Role-Based Training, Insider Threat Awareness. Security awareness training platforms (e.g., KnowBe4, Proofpoint), phishing simulation tools, e-learning modules, compliance tracking software.
Audit & Accountability (AU)	Security Information and Event Management (SIEM) tools (e.g., Splunk, Microsoft Sentinel), centralized log management (e.g., Graylog, ELK Stack), log retention solutions, audit trail software.
Configuration Management (CM)	Configuration management tools (e.g., Ansible, Puppet, Chef), vulnerability scanning tools (e.g., Nessus, Qualys), patch management systems (e.g., WSUS, Ivanti).
Identification & Authentication (IA)	MFA solutions (e.g., Duo, Auth0), biometric authentication, smart card systems, password management tools (e.g., LastPass, 1Password), certificate-based authentication.

Contact Us 888-951-7675 www.capeendeavors.com info@capeendeavors.com

Mapping NIST 800-171 to Real-World Implementation

CAPE ENDEAVORS

Control Family	Example Technologies/Implementations
Incident Response (IR)	Incident response platforms (e.g., ServiceNow, PagerDuty), threat hunting tools (e.g., CrowdStrike Falcon, Palo Alto Cortex XDR), ticketing systems (e.g., Jira), forensic analysis tools (e.g., EnCase).
Maintenance (MA)	Remote monitoring and management (RMM) tools (e.g., SolarWinds, ConnectWise), automated maintenance scheduling software, secure remote access solutions (e.g., BeyondTrust).
Media Protection (MP)	Data encryption tools (e.g., VeraCrypt, BitLocker), secure file transfer protocols (e.g., SFTP), media sanitization software (e.g., DBAN, CCleaner), removable media controls.
Physical Protection (PE)	Physical access control systems (e.g., keycard systems, biometric locks), surveillance systems (e.g., CCTV), environmental controls (e.g., fire suppression, HVAC monitoring).
Risk Assessment (RA)	Risk assessment tools (e.g., RiskLens, Archer), vulnerability management platforms (e.g., Tenable, Rapid7), threat modeling tools, penetration testing tools (e.g., Metasploit).
Security Assessment (CA)	Security assessment tools (e.g., OpenVAS, Burp Suite), continuous monitoring solutions (e.g., SolarWinds Security Event Manager), compliance management software (e.g., OneTrust).

Contact Us 888-951-7675 www.capeendeavors.com info@capeendeavors.com

Mapping NIST 800-171 to Real-World Implementation

CAPE ENDEAVORS

Control Family	Example Technologies/Implementations
System & Communications Protection (SC)	Endpoint detection and response (EDR) tools (e.g., SentinelOne, Carbon Black), network firewalls (e.g., Cisco, Fortinet), VPNs, encryption tools (e.g., TLS, AES-256, FIPS 140-2 validated modules).
System & Information Integrity (SI)	Antivirus and anti-malware solutions (e.g., Malwarebytes, McAfee), integrity monitoring tools (e.g., Tripwire), software whitelisting, intrusion detection systems (IDS) (e.g., Snort, Suricata).
Personnel Security (PS)	Background check services, employee monitoring software, access termination workflows, insider threat detection tools (e.g., Varonis, Securonix).

Notes:

- Scope: The matrix focuses on practical technologies and methods that align with NIST 800-171's 110 security requirements, emphasizing Controlled Unclassified Information (CUI) protection.
- Flexibility: Implementations vary by organization size, budget, and infrastructure (e.g., cloud vs. on-premises). The listed technologies are examples, not exhaustive.
- Compliance: Technologies must be configured to meet specific NIST 800-171 requirements—such as FIPS 140-2 validated cryptography for SC controls or 90-day log retention for AU controls—and, if cloud services are used, the environment must be FedRAMP-authorized (Moderate or High) when handling Specified CUI.
- Sources: This matrix is informed by NIST 800-171 documentation, industry practices, and cybersecurity vendor tools commonly referenced in compliance discussions.

Contact Us 888-951-7675 www.capeendeavors.com info@capeendeavors.com

Scoping Your Environment for CUI

Scoping is one of the most critical—and often misunderstood—steps in preparing for CMMC certification. Done wrong, it drives up costs or leaves CUI exposed. Scoping isn't just listing systems—it's mapping how CUI is created, received, stored, transmitted, and accessed.

Start with the data flow: use interviews, document reviews, and scanning tools to trace CUI across email, file shares, cloud apps, mobile devices, servers, and backups.

Know the five asset categories defined by CMMC:

1. **CUI Assets** – Store, process, or transmit CUI
2. **Security Protection Assets** – Provide security functions (e.g., firewalls, antivirus)
3. **Contractor Risk Managed Assets** – Don't handle CUI but are connected and managed through risk decisions
4. **Specialized Assets** – Require tailored security measures (e.g., lab equipment, OT systems)
5. **Out-of-Scope Assets** – Fully isolated with no CUI interaction or connection

A device is in scope if it is used to create, store, transmit, process, or view CUI. This includes laptops, desktops, smartphones, or even monitors that display CUI content. If CUI touches it—it's in scope.

Minimize your scope wherever possible.
Limit the systems and users interacting with CUI using segmentation techniques like secure enclaves, virtual desktops, or centralized document repositories. Smaller scopes reduce complexity and cost while strengthening security posture.

Define and document your boundaries.
Assessors require clear evidence of what is in and out of scope. Provide current network diagrams that show trust zones, data flows, access controls, and boundary protections. Documentation should be detailed and traceable to the scoping rationale

Additional Resources:
Where's My CUI?
Misclassified CUI: How Small Mistakes Create Big Risks for Defense Contractors

Contact Us 888-951-7675 www.capeendeavors.com info@capeendeavors.com

Build vs. Buy: Internal vs. Managed Secure Enclave

Implementing a CMMC-compliant IT environment is a strategic decision that hinges on cost, expertise, time, and risk tolerance. Contractors must choose between building an internal secure enclave from scratch or leveraging a managed solution.

Building Internally

High Upfront Capital: Organizations must purchase or configure infrastructure like firewalls, endpoint protection platforms, centralized logging, GRC tools, and email encryption—all aligned to NIST 800-171 requirements.

Cybersecurity Staffing: Internal builds require in-house cybersecurity experts who understand federal compliance frameworks. Many small to mid-sized firms struggle to hire or retain cleared professionals with this skillset.

Customization vs. Complexity: Internal teams can tailor environments, but they must also write, maintain, and update detailed documentation such as System Security Plans (SSPs), Plans of Action and Milestones (POA&Ms), and incident response protocols. This documentation must stand up to scrutiny during a C3PAO assessment.

Managed Secure Enclave

Turnkey Infrastructure: Providers like Cape Endeavors deliver pre-configured environments purpose-built to meet all 110 NIST SP 800-171 controls, hosted in government-authorized clouds (e.g., Microsoft GCC High). **See Cape Endeavors Azure GCC & GCCH Secure Enclave Services – What You Need to Know**

·**Operational Support**: Enclave providers manage patching, logging, backup, and incident response services—all mapped to CMMC requirements. This helps contractors demonstrate continuous monitoring and corrective action.

Accelerated Compliance: Managed solutions typically include policy templates, mapped controls, and artifacts necessary for audit readiness. This drastically reduces time-to-certification and supports ongoing compliance as requirements evolve.

Build vs. Buy: Internal vs. Managed Secure Enclave

CAPE ENDEAVORS

Build vs Buy	Build Internally	Managed Secure Enclave
Initial Cost	High – Purchase Infrastructure, Software, Tools	Moderate – Subscription-Based Model
Time to Deploy	Slow - 6–12 Months or Longer	Fast – Often Under 90 days
Internal Staff Requirement	Significant – Multiple Roles Needed	Minimal – Provider Manages Infrastructure
CMMC Expertise Required	Yes – Must Be Hired or Contracted	No – Provider Brings Certified Expertise
Documentation Burden	High – All Plans, Policies Written In-House	Low – Pre-written templates and frameworks
Maintenance & Monitoring	In-House IT/SecOps Team Required	Included in Service Agreement
Audit Readiness	Dependent on Internal Preparation	High – Documentation and Evidence Provided
Scalability	Variable – May Require Major Upgrades	Easy – Scales with Organization
Long-Term Cost	High – Ongoing Staffing and Updates	Predictable – Lower Total Cost of Ownership

Contact Us 888-951-7675 www.capeendeavors.com info@capeendeavors.com

SSP & POA&M Frameworks

The **System Security Plan (SSP)** is a cornerstone of NIST SP 800-171 and CMMC compliance. It documents how your organization meets each security requirement, describes your system environment, and defines how and where Controlled Unclassified Information (CUI) is handled. An effective SSP must be current, complete, and accurately reflect your operating environment. A well-prepared SSP typically includes:

- **Introduction & Scope**: Overview of the organization, including contract references, CUI categories in use, and the scope of the SSP.
- **System Environment:** Description of IT systems, platforms, applications, and infrastructure that process, store, or transmit CUI.
- **CUI Flow Diagrams:** Visual maps showing where CUI enters, how it flows through, and how it exits your systems or cloud environments.
- **Control Implementation Details**: For each of the 110 NIST SP 800-171 controls, describe how it is satisfied—naming specific technologies, configurations, policies, and procedures in place.

Cloud Service Requirements Based on CUI Type

The type of CUI your organization handles—**CUI Basic or CUI Specified**—directly impacts the type of cloud environment that may be used.

- For **CUI Basic**, cloud services must be FedRAMP Moderate or higher.
- For **CUI Specified**, which involves stricter safeguarding and dissemination controls, Microsoft **GCC High (GCCH)** or equivalent U.S.-sovereign cloud environments are required. Selecting the wrong cloud environment can invalidate your compliance efforts and introduce significant risk.

SSP & POA&M Frameworks

The **Plan of Action and Milestones (POA&M)** accompanies the SSP and is used to document deficiencies in control implementation, along with a path to remediation. Under CMMC 2.0, POA&Ms are allowed only under specific conditions.

Eligibility for POA&Ms in CMMC 2.0:

- **Level 1:** No POAMs allowed. All 17 controls from FAR 52.204-21 must be fully implemented at the time of assessment.
- **Level 2 (based on NIST SP 800-171)** POAMs are allowed for non-critical requirements under specific conditions:
  - Most 1-point controls are eligible, except five specific 1-point controls that must be fully implemented (these are referenced in DoD briefings but not individually named in the public rule).
  - Control 3.13.11 (FIPS-validated encryption) is the only 5-point control eligible for a POA&M if partially implemented.
  - 3-point and other 5-point controls are ineligible—they must be fully implemented.

If Conditional Certification is granted, organizations have **180 days** to resolve all POA&M items and complete a Delta Assessment. Failure to achieve full compliance within that period results in revocation of certification.

Best Practices for POA&M Management:

- Develop detailed remediation plans with actionable steps and assigned personnel.
- Set realistic milestones to meet the 180-day deadline.
- Conduct regular progress reviews (e.g., monthly or bi-weekly).
- Use compliance tools to track and document POAM items.
- Prepare comprehensive documentation for the closeout assessment to ensure all evidence is accessible to assessors

⚠️ **Important:** POA&M are no longer a broad workaround. Their use is strictly limited under the final rule, and the affirming official who signs off on compliance assumes personal accountability for its accuracy and completeness.

Additional Resources:

NIST SSP Template
NIST POAM Template

Assessment Preparation Checklist

Preparing for a CMMC assessment requires a disciplined and thorough approach. Contractors should begin months in advance and ensure both documentation and operational practices align with NIST SP 800-171 and the target CMMC level.

- **Conduct a gap analysis aligned to NIST 800-171**: Identify which of the 110 controls are fully, partially, or not implemented. Use this analysis to prioritize corrective actions.
- **Complete or update your SSP and POAM**: Ensure your documentation reflects your current environment and includes accurate implementation narratives and remediation plans.
- **Ensure all personnel have signed acceptable use policies (AUPs)**: AUPs should define system usage rules and be re-signed annually to demonstrate user accountability.
- **Train users on incident reporting and security practices**: Conduct training on phishing identification, insider threat recognition, and how to report incidents through proper channels.
- **Validate logging, alerting, and incident response procedures**: Simulate events and verify that logs are collected, correlated, and actionable by your monitoring team or service provider.
- **Perform internal mock assessments (or hire a third party)**: Simulate the assessment process using CMMC 2.0 assessment guides. Validate evidence, interview readiness, and correct any discrepancies found.

Assessment Preparation Resources:

CyberAB - **CMMC Assessment Process v2.0**
DoD CIO - **CMMC Assessment Guide – Level 2 | Version 2.13**
CMMC Info - **NIST SP 800-171 Basic Self Assessment scoring template**

About Cape Endeavors

Cape Endeavors is a fully comprehensive Managed CMMC Secure Enclave Provider that offers consulting services to the defense industrial base. Our team of Certified CMMC Assessors (CCPs) and Certified CMMC Professionals (CCPs) delivers practical, audit-proven solutions. We offer:

- Custom secure enclave design
- CUI mapping and cloud tenant hardening
- User management, security monitoring, and compliance maintenance
- CUI migration and spillage response
- CMMC assessment preparation and representation

From strategy to execution, we ensure your environment is secure, compliant, and audit-ready with technical expertise and regulatory precision.

We provide the expertise you can count on, **contact us** today to learn more!

Contact Us 888-951-7675 www.capeendeavors.com info@capeendeavors.com