

Preparing for CMMC Phase 2: A Practical Guide for Government Contractors

Phase 2 of the Cybersecurity Maturity Model Certification (CMMC) is no longer something contractors can afford to think about later. With the implementation date now announced for [Date], defense contractors and subcontractors now have a clear timeline and a strong reason to move quickly. The good news is that preparing for Phase 2 does not have to feel overwhelming. By understanding what is changing, identifying where your organization stands today, and building the right documentation, evidence, and technology foundation, contractors can put their team in a much stronger position before Phase 2's self and third-party assessment requirements begin showing up in contracts.

What PHASE 2 Means

Phase 1 focused primarily on self-assessments and contractor attestations. **Phase 2 introduces a significant change for many organizations handling CUI by requiring independent assessments conducted by Certified Third-Party Assessment Organizations (C3PAOs) rather than relying solely on self-attestation.** Organizations seeking Level 2 certification must demonstrate that required NIST SP 800-171 controls are implemented and supported with verifiable evidence.

Organizations that process, store, or transmit CUI under DoD contracts are most likely to be affected by Phase 2. Prime contractors, technology providers, engineering firms, manufacturers, logistics providers, and many members of the Defense Industrial Base (DIB) will likely face the greatest impact because certification readiness becomes directly tied to contract eligibility and supply chain participation. Even if implementation dates shift, organizations that wait for final announcements may find themselves competing for limited assessor availability and remediation resources.

What Happens If You're Not Ready

Organizations that fail to prepare face more than just compliance challenges. Without the required certification level, contractors may become ineligible for certain DoD contracts or may be unable to continue supporting programs that require CMMC verification. Prime contractors may also hesitate to engage subcontractors that cannot demonstrate readiness, creating downstream revenue and partnership risks.

Operationally, waiting until the last minute often leads to rushed security projects, unexpected remediation costs, staffing challenges, and assessment delays. Competitive risks can be equally significant. Contractors that achieve readiness early can continue pursuing opportunities while competitors scramble to close security gaps. Organizations that inaccurately represent their cybersecurity posture may also face contractual and legal exposure related to cybersecurity attestations and compliance claims.

Technology Considerations for Contractors:

Why CallTower

CMMC readiness is not solely a policy exercise; technology architecture matters. Contractors need the right communication and collaboration tools to support the security expectations of government work. This is where CallTower can help. CallTower provides Microsoft Teams Direct Routing for GCC High, giving contractors a practical way to add enterprise voice and calling to their Microsoft 365 GCC High environments.

While CallTower does not replace the work of a C3PAO, consultant, or internal security team, and our solutions do not make an organization CMMC compliant on their own, CallTower does provide a secure, reliable, compliant-ready communications foundation to make achieving CMMC compliance easier for government contractors, all while modernizing collaboration and voice communications.

Purpose-Built for Government-Focused Cloud Environments & CUI

CallTower's Teams GCC High offering is designed to operate in environments where CUI is handled and supports federal security frameworks like FedRAMP, ITAR, and NIST 800-171. This allows contractors to align their communications environment with broader compliance objectives.

Enterprise Cloud Voice Inside GCC High

CallTower delivers Direct Routing within GCC High, allowing contractors to centralize collaboration and voice into a single environment. This reduces the complexity of maintaining multiple platforms and reduces the risks associated with disconnected systems.

Proven GCC High Expertise Reduces Deployment Risk

CallTower has been delivering Direct Routing in GCC High since 2019 and has developed implementation expertise specifically around voice enablement in government cloud environments. This experience helps contractors avoid costly deployment mistakes and accelerate adoption.

Lower Infrastructure Burden & Operational Complexity

CallTower's cloud-based Direct Routing eliminates the need for traditional infrastructure while simplifying management and ongoing operations. This allows contractors to dedicate more time and resources to mission-focused initiatives.

24/7/365 Monitoring and Support

CallTower offers continuous monitoring through our Network Operations Centers along with 24/7/365 support. This reduces the operational burden on internal IT teams and ensures maximum uptime when communications are critical.

How to Prepare for CMMC Phase 2

Determine Your Required CMMC Level

Before investing in remediation efforts, organizations must identify which CMMC level applies to their contracts and business operations.

The Three CMMC Levels

LEVEL 1

Focused on safeguarding Federal Contract Information (FCI).

LEVEL 2

Focused on protecting Controlled Unclassified Information (CUI) and aligning with NIST SP 800-171 requirements.

LEVEL 3

Designed for contractors supporting highly sensitive programs and may require government-led assessments.

How to Identify Your Requirements

Review existing DoD contracts and solicitations.

Identify whether your organization handles FCI, CUI, or both.

Examine DFARS clauses included in contracts.

Recommended to coordinate with contracting officers and prime contractors.

Document where sensitive information is stored, processed, or transmitted.

Mistakes Contractors Should Avoid

Assuming all contracts require the same certification level.

Underestimating the scope of systems that handle CUI.

Ignoring subcontractor and supply-chain requirements.

Waiting until certification requirements appear in a contract before preparing.

How to Prepare for CMMC Phase 2

Conduct a Readiness Assessment

A readiness assessment helps organizations understand where they stand before pursuing a formal evaluation.

Measuring Current Control Implementation

- Review current security controls against applicable CMMC requirements.
- Evaluate policy maturity and operational execution.
- Assess technical controls, monitoring capabilities, and user practices.
- Validate that security processes are consistently followed.

Performing a Gap Analysis

- Compare current controls to required controls.
- Identify missing documentation.
- Review technical configurations and system boundaries.
- Confirm evidence can be produced for each control.

Prioritizing Potential Risk Deficiencies

- Multi-factor authentication gaps.
- Weak access control practices.
- Missing audit logging.
- Incomplete incident response processes.
- Unmanaged endpoints or unsupported systems.
- Lack of documented procedures.

How to Prepare for CMMC Phase 2

Build an Assessment-Ready Documentation Package

Many organizations discover that documentation, not technology, becomes their greatest obstacle during an assessment.

Typical Policies & Procedures to Support Objectives



Information security policies



Risk management documentation



Access control procedures



Training and awareness procedures



Incident response plans



Vendor and third-party management policies



Configuration management policies

Evidence Assessors May Expect

01

System Security Plans (SSPs)

02

Network diagrams

03

Security configurations

04

Audit logs

05

Vulnerability assessment reports

06

Risk registers

07

Training records

08

Incident response testing results

Recommended Evidence-Management Practices



Track updates and approvals.



Maintain version control.



Define document ownership.



Create a single centralized document repository.



Ensure leadership visibility into readiness status.

How to Prepare for CMMC Phase 2

Prepare for a C3PAO Assessment

Organizations should treat preparation for a formal assessment as a structured project, not a final compliance checkpoint.

What a C3PAO Does

A C3PAO is an accredited assessment organization authorized to perform Level 2 certification assessments and verify implementation of required controls. Assessment results are formally documented and submitted through official CMMC processes.

How Assessments Typically Work

- Assessment scope is established.
- Documentation is reviewed.
- Interviews are conducted.
- Technical evidence is validated.
- Findings are documented.
- Any allowable remediation activities are addressed according to program rules.

Potential Issues Found During Assessments

- Incomplete SSPs.
- Policies that exist but are not operationalized.
- Missing evidence for implemented controls.
- Poor asset inventory management.
- Inadequate user training records.
- Weak documentation of recurring security activities.

Address Organizational Readiness

Technology and documentation alone do not produce successful assessments.
Organizational commitment is equally important.

Executive Leadership Best Practices

- ✓ Establish cybersecurity as a business priority.
- ✓ Fund remediation activities.
- ✓ Assign accountability for CMMC readiness.
- ✓ Review readiness metrics regularly.
- ✓ Understand contractual risks associated with non-compliance.

Employee Awareness & Training

- ✓ Train employees on CUI handling requirements.
- ✓ Conduct recurring security awareness training.
- ✓ Reinforce reporting procedures for incidents.
- ✓ Include personnel whose roles fall within assessment scope or involve FCI/CUI.

Establishing Continuous Compliance

- ✓ Perform recurring internal assessments.
- ✓ Review controls regularly.
- ✓ Maintain current documentation.
- ✓ Monitor emerging regulatory changes.
- ✓ Treat CMMC as an ongoing operational program rather than a one-time certification effort.