CMMC Quick Start Guide

A practical roadmap for scoping, NIST 800-171 alignment, and assessment readiness

Prepared by Jacobian Engineering | 2026-02-09

This quick start guide is for informational purposes only and does not constitute legal advice.

Executive Summary

CMMC is the Cybersecurity Maturity Model Certification used in the defense industrial base. It is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that contractors handle for the Department of Defense. CMMC readiness requires more than policy writing. It requires technical controls, documented processes, and evidence that the controls operate.

This quick start guide explains how to scope CMMC work, build a realistic implementation plan, and prepare the documentation and evidence that assessments expect. The focus is practical steps that help small and mid-sized contractors meet requirements without creating unnecessary overhead.

Background and who CMMC applies to

CMMC requirements are tied to DoD contracts. If your contract involves handling FCI or CUI, the contract may include specific cybersecurity requirements. CMMC organizes those requirements into maturity levels and requires contractors to demonstrate implementation.

- **FCI:** Information provided by or generated for the government under contract that is not intended for public release.
- **CUI:** Sensitive information that requires safeguarding or dissemination controls, even though it is not classified.
- **Defense industrial base:** Prime contractors and subcontractors that provide products or services to the DoD.
- **Core foundation:** Many CMMC requirements align with NIST SP 800-171, which focuses on protecting CUI in non-federal systems.

Your first step is to understand whether you handle FCI, CUI, or both. That decision influences scope, architecture, and what level of controls you must implement.

CMMC levels in plain language

CMMC 2.0 is commonly described in three levels. Level 1 focuses on foundational practices for protecting FCI. Level 2 focuses on protecting CUI and is aligned to NIST SP 800-171 practices. Level 3 is intended for higher-risk programs and adds additional requirements beyond 800-171.

- **Level 1:** Basic cyber hygiene practices. Often relevant for contractors that handle only FCI.
- **Level 2:** Practices aligned to NIST SP 800-171 for protecting CUI. This is the most common target for contractors with CUI.
- **Level 3:** Advanced practices for selected high-risk programs. Requirements can include additional controls beyond the baseline.

Contracts and flow-down requirements determine what level you need. Many subcontractors must meet the same level as the primes they support, especially when CUI is involved.

Scope and architecture decisions

CMMC scope is driven by where CUI lives and how it flows. If CUI is spread across email, shared drives, laptops, and multiple cloud accounts, scope grows quickly. Many contractors reduce scope by creating a defined enclave where CUI is handled and by limiting where CUI can be stored or processed.

Build a clear CUI boundary

- **Identify CUI touchpoints:** Contracts, engineering drawings, support tickets, email, file shares, and collaboration tools.
- **Map data flows:** How CUI enters, where it is processed, who accesses it, and where it leaves the organization.
- **Choose an enclave approach:** A separate environment for CUI can reduce scope and make evidence more consistent.
- **Control endpoints:** If endpoints access CUI, they often become in scope. Use managed devices and strong access controls.
- **Document decisions:** Scope decisions should be documented so assessors can follow your logic.

Quick start roadmap for CMMC readiness

CMMC readiness is a combination of technical implementation, documentation, and evidence. The roadmap below is designed for organizations targeting CMMC Level 2, since it is the most common requirement for CUI handling. Adjust the depth based on your contract requirements.

Phase	Outcomes	What to produce
Phase 1: CUI discovery and scoping (Weeks 1 to 3)	Clear CUI boundary and inventory	CUI data flow map, asset inventory, boundary diagram, decis
Phase 2: Gap assessment to NIST 800-171 (Weeks 2 to 5)	Known gaps and remediation plan	Gap assessment, System Security Plan outline, POA&M draf
Phase 3: Implement controls and documentation (Weeks 5 to 16)	Controls operating and evidence collected	Policies and procedures, technical safeguards, configuration
Phase 4: Evidence and readiness review (Weeks 12 to 20)	Assessment-ready evidence set	Completed SSP, updated POA&M, evidence library mapped t
Phase 5: Assessment planning (Timing varies)	Assessment readiness	Assessment coordination, access plan for assessors, final rev

Phase 1: CUI discovery and scoping

1. Interview contract and program owners to confirm where CUI is created and stored.
2. Map where CUI flows through systems and vendor tools. Include endpoints and collaboration platforms.
3. Decide how you will contain CUI. A defined enclave with controlled access often reduces scope and improves consistency.
4. Create a boundary diagram and an asset inventory that will support your System Security Plan.

Phase 2: Gap assessment and planning

A gap assessment against NIST SP 800-171 identifies what practices are missing, weak, or undocumented. Use the results to build a prioritized plan. The System Security Plan (SSP) describes your environment and how you meet each requirement. The Plan of Action and Milestones (POA&M;) tracks remaining gaps and remediation.

Phase 3: Implement controls

Implementation often requires improvements in identity, endpoint management, logging, vulnerability management, configuration control, and incident response. Keep changes tracked and approved so you can produce evidence of how controls were implemented and how they operate.

- **Access control:** Least privilege, multi-factor authentication, privileged account controls, and regular access reviews.
- **Endpoint security:** Managed devices, encryption, patching routines, and endpoint protection.
- **Configuration management:** Secure baselines, change control, and documented exceptions.
- **Logging and monitoring:** Central logs for key systems and documented review and alert handling.
- **Incident response:** Response plan, roles, and evidence of exercises and improvements.
- **Training:** Security awareness training with content relevant to handling CUI.

Phase 4: Evidence and readiness review

Assessments focus on evidence. Build an evidence library mapped to each practice. Include screenshots, tickets, reports, and signoffs. Run an internal readiness review to find gaps before an external assessment.

Phase 5: Assessment planning

Plan how assessors will see evidence and how they will access systems. Prepare staff for interviews and ensure roles are clear. A calm, organized assessment experience often reflects a well-run program.

Common CMMC pitfalls

- **Uncontrolled CUI sprawl:** If CUI is scattered across tools, scope grows and evidence becomes inconsistent. Containment through an enclave or controlled workflows reduces burden.
- **Documentation without implementation:** A policy does not prove a control. You need technical configuration, operational routines, and evidence.
- **Weak asset inventory:** You cannot protect what you cannot list. Inventory systems, endpoints, and users that touch CUI.
- **Ignoring subcontractor and vendor impact:** If vendors touch CUI, they can affect your compliance posture. Document responsibilities and evaluate vendor controls.

- **POA&M; treated as a parking lot:** A POA&M; needs owners, dates, and active tracking. Unmanaged gaps can block readiness.

CMMC work becomes easier when CUI is handled in a controlled way and the evidence process is built into normal operations.

How Jacobian Engineering helps

Jacobian Engineering supports defense contractors through CMMC preparation and NIST 800-171 implementation. The approach blends compliance guidance with hands-on engineering to implement controls in real environments, including cloud and hybrid systems.

- **Scope and enclave design:** CUI data flow mapping, boundary definition, and secure enclave architecture to reduce scope.
- **Gap assessment:** Practical assessment against NIST 800-171 with a prioritized remediation plan.
- **SSP and POA&M; development:** Documentation support that reflects real controls and creates a clear audit story.
- **Control implementation:** Endpoint hardening, logging and monitoring, access management, and incident response program support.
- **Security testing:** Penetration testing and validation of remediation where appropriate.

CMMC quick start FAQ

How do we know if we have CUI?

Your contracts, statements of work, and communications with primes typically indicate whether CUI is involved. Program owners and contract managers should confirm markings and data handling expectations. Treat uncertainty seriously and document what you learn.

Is CMMC the same as NIST 800-171?

Many CMMC requirements for protecting CUI align to NIST SP 800-171 practices. CMMC also adds an assessment and certification model tied to contracts. Your implementation work often begins with 800-171 alignment.

What is the first step we should take?

Map where CUI could exist and how it flows. That scope work prevents wasted effort and helps you choose an enclave approach if it makes sense.

Can we reduce scope with a separate environment?

Yes, many contractors use a controlled enclave for CUI handling. The key is enforcing that CUI stays inside the boundary through technical controls and training.

Conclusion

CMMC readiness is achievable when you contain CUI, implement controls that protect the enclave and endpoints, and produce evidence that shows controls operate consistently. Start with CUI discovery and scoping, then build the SSP and remediation plan alongside technical implementation. A structured approach reduces risk and improves your ability to compete for DoD work.