Cybersecurity Maturity Model Certification (CMMC)

Cisco Partner
https://cs.co/1page

The **Cybersecurity Maturity Model Certification** (CMMC) is a Department of Defense (DoD) framework designed to verify that contractors protect sensitive information. It ensures controls are in place to safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) within the Defense Industrial Base (DIB).

Benefits:

Contractual Eligibility: Compliance is essential for winning DoD contracts, as certification confirms a contractor's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Enhanced Cybersecurity: Implementation of CMMC controls (like NIST SP 800-171) improves security posture, reducing the risk of data breaches and costly downtime.

Competitive Advantage: Certified organizations are viewed as more secure and reliable partners within the Defense Industrial Base (DIB), opening up new business opportunities.

Improved Efficiency: The process helps streamline IT systems, consolidate security tools, and improve staff productivity by clarifying security workflows.

Reduced Risk and Liability: Proactive compliance reduces the danger of potential criminal actions, contract losses, and fines for non-compliance.

Streamlined Compliance Processes: Programs like those in Michigan offer targeted, reduced-cost assistance for small-to-medium businesses to meet these standards.

CMMC Certification Process:

CMMC self-assessment. All DIB organizations, regardless of their required CMMC level, must conduct a thorough self-assessment to evaluate their current cybersecurity maturity practices against CMMC requirements and identify areas for improvement. For Level 1 and a subset of organizations requiring Level 2, an annual self-assessment will be sufficient to satisfy CMMC requirements.

Third-party assessment. Organizations requiring Level 2 or Level 3 must pass a third-party assessment to certify compliance with CMMC requirements. For Level 2, the assessment is conducted by a C3PAO (CMMC Third-Party Assessor Organization), while Level 3 requires an assessment by the DIBCAC, the Defense Industrial Base Cybersecurity Assessment Center of the DoW. Marine Corps, Air Force and entities such as Space Force, the U.S. Coast Guard and the National Guard. In 2025, this was renamed the “Department of War”.

CMMC certification. If the assessment is successful, organizations receive their CMMC certification. This certification is valid for three years, after which organizations must undergo re-assessment to maintain their CMMC status.

Get ready for the assessment. When ready for the assessment, ensure that everything is up to date and easily accessible for the assessment team.

CMMC Levels:

Level 1: Foundational (Self-Assessment)
- Purpose: Protects Federal Contract Information (FCI).
- Requirements: 15 basic cyber hygiene practices from FAR clause 52.204-21.
- Assessment: Annual self-assessment required.

Level 2: Advanced (Self-Assessment or C3PAO)
- Purpose: Protects Controlled Unclassified Information (CUI).
- Requirements: 110 security controls derived from NIST SP 800-171 Rev 2.
- Assessment: Third-party assessment (C3PAO) every 3 years is required for most; some non-prioritized CUI contracts may allow self-assessment.

Level 3: Expert (DIBCAC Assessment)
- Purpose: Protects CUI on high-priority DoD programs from advanced persistent threats (APTs).
- Requirements: Based on NIST SP 800-171 and a subset of NIST SP 800-172, including 110+ practices.
- Assessment: Government-led assessment (DIBCAC) every 3 years.

FAQs:

Q: Will CMMC requirements flow down to subcontractors?
A: Yes, requirements will flow to subcontractors as outlined in 32 CFR 170.23.

Q: How frequently will assessments be required?
A: Level 1 self-assessments will be required on an annual basis, and CMMC Levels 2 and 3 will be required every 3 years.

Q: How will the DoD implement CMMC?
A: The Department will implement CMMC requirements in 4 phases over a three-year period, as described in 32 CFR 170.3(e).

Resources:

FAQ		
Cisco Frameworks & Certs	What is CMMC	CMMC Cisco Blog
Framework Foundations	Splunk for CMMC	Documentation
Quick Start Guide	CMMC Solution Brief	Defense.gov