corsica technologies

IT Compliance Services

CMMC Compliance Cheat Sheet

Enterprise Managed Services | Strategic IT & Cybersecurity | Compliance | AI + Digital Transformation

What is CMMC?

CCMMC stands for "Cybersecurity Maturity Model Certification" and is a unifying standard for the implementation of cybersecurity across the Department of Defense (DoD) supply chain. CMMC compliance encompasses multiple levels of cybersecurity maturity that range from Basic to Advanced, ensuring that all contractors handling government information are adequately protecting it.

What does it mean?

With the publication of the 48 CFR part 204 CMMC Acquisition final rule on September 10, 2025, CMMC requirements are no longer optional. The rule will be implemented in a phased approach over three years, starting on November 10, 2025. This means that new DoD contracts will begin to include CMMC requirements, and contractors will need to be certified at the appropriate level prior to being awarded a contract. These requirements are "pre-award," meaning that contractors must be certified before they can be awarded a contract. Additionally, after November 10, 2025, all contract renewals will require the appropriate level of CMMC compliance, even if the original contract was awarded before CMMC was required.

What are the compliance levels and what do they mean?

The CMMC 2.0 model has three levels of compliance, each with its own set of requirements and assessment procedures. The level of compliance required for a specific contract depends on the sensitivity of the information being handled.

CMMC Level	Desired Result	Requirements	Assessment
Level 1	Basic Cyber Hygiene for FCI	15 security requirements from FAR 52.204-21	Annual Self-Assessment
Level 2	Broad Protection of CUI	110 security requirements from NIST SP 800-171 Rev. 2	Self-Assessment or C3PAO Assessment every 3 years (as specified in solicitation)
Level 3	Higher-Level Protection of CUI	110 requirements from NIST SP 800-171 Rev. 2 + 24 selected requirements from NIST SP 800-172	Government-led assessment by DIBCAC every 3 years

How do companies become CMMC compliant?

The first step in becoming CMMC compliant is to conduct a CMMC Compliance Gap Analysis. This analysis is based on a company's required CMMC level and will reveal any gaps in their cybersecurity controls and processes that must be addressed in order to meet compliance standards. Depending on the required CMMC level, a company may need to undergo a self-assessment, a third-party assessment by a Certified Third-Party Assessment Organization (C3PAO), or a government-led assessment by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

What is the Final Rule?

The DoD CMMC Final Rule took effect on December 16, 2024, establishing a framework for cybersecurity requirements in defense contracts. While the rule is in effect, Phase 1 implementation—requiring contractors to meet specific CMMC levels—begins on November 10, 2025, following the publication of the related DFARS amendment. This rollout strengthens protections for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) across the DoD supply chain.

What do DoD contractors need to do today?

The first thing a DoD contractor must do today is self-assess against the CMMC requirements for their target CMMC level. For most contractors, this will be Level 2, which requires compliance with the 110 controls in NIST SP 800-171. Contractors should also begin preparing for the required assessments, whether it is a self-assessment or a third-party assessment. It is also critical to stay informed about the CMMC implementation timeline and how it will affect your current and future contracts.

Can we become CMMC-certified through a self-assessment?

While CMMC certification cannot be achieved through self-assessment, compliance with Level 1 and some Level 2 contracts can be met with a self-assessment. For Level 1, an annual self-assessment is required. For Level 2, the contract will specify whether a self-assessment or a third-party assessment by a C3PAO is required. CMMC Level 3 requires a government-led assessment by DIBCAC.

Confidently meet compliance requirements with a CMMC Compliance Consultation.

As a NIST Consultant, we help Department of Defense (DoD) contractors throughout the U.S. implement the NIST 800-171 cybersecurity framework in order to comply with DFARS and prepare for an upcoming CMMC audit.

REACH OUT TODAY!

> **Can't say enough about how helpful Corsica Technologies has been** to Scientific Sales' efforts to meet CMMC cybersecurity requirements that will allow us to continue serving our government customers."

★★★★★

Donald Evans | *VP of Operations* | *Scientific Sales*

corsica technologies

10-25

corsicatech.com | sales@corsicatech.com | (855) 411-3387