corsica technologies

CMMC Compliance Cheat Sheet

What is CMMC?

CMMC stands for "Cybersecurity Maturity Model Certification" and is a unifying standard for the implementation of cybersecurity among Department of Defense contractors. CMMC encompasses multiple levels of cybersecurity practices from Basic Cyber Hygiene at Level 1 to Advanced/Progressive Practices at Level 5. CMMC practices are mostly technical in nature. CMMC's processes start at Level 2 "Documented" and proceed to Level 5 "Optimizing". Practices and Processes across the 17 CMMC domains are cumulative in nature and are used to determine the maturity level of an organization. For example, an organization must meet all practice requirements at level 1 and all practice and process requirements at level 2 to be certified at CMMC Level 2.

What does it mean?

By 2025, all new DoD contracts will contain CMMC requirements. Most contractors will be required to meet Level 1 requirements – the minimum necessary for Federal Contract Information. These requirements are "pre-award" which means that contractors will need to be certified at the appropriate level prior to being awarded a contract. All practices and processes must be determined to be implemented by a 3PCAO for the organization to be certified at that level.

How do companies become CMMC compliant?

The first step is conducting a CMMC Compliance Gap Analysis. This analysis is based on a company's required CMMC level and will reveal gaps in their cybersecurity controls and processes that must be addressed in order to meet that level's requirements.

What are the compliance levels and what do they mean?

CMMC Level	Desired Result	Requirements
Level 1	Basic Cyber Hygiene	17 practices of NIST 800-171 Rev. 1
Level 2	Intermediate Cyber Hygiene	48 practices of NIST 800 800-171 Rev. 1 plus 7 other new practices
Level 3	Good Cyber Hygiene	Final 45 practices of NIST 800-171 Rev. 1, plus 20 other new practices for a total of 130 practices.
Level 4	Proactive	13 practices of NIST 800-171 Rev. B plus 13 other new practices
Level 5	Advanced/Progressive	All practices, including the remaining 5, of NIST 800-171 Rev. B plus 11 other new practices

CMMC Compliance Cheat Sheet

corsica technologies

What is the Interim Rule?

CMMC will not be fully implemented until September 2025. The DoD has issued the CMMC Interim Rule consisting of three regulations: DFARS 252.204-7019, 252.204-7020, and 252.204-7021. The Interim Rule requires that contractors continue to be NIST 800-171 compliant via 252.204-7019. The 252.204-7020 rule requires primes to make sure contractors have submitted a SPRS score prior to contract award. The 252.204-7020 regulation allows the government to "hand pick" the organizations that will be subject to CMMC prior to 2025.

What do DoD contractors need to do today?

The first thing a DoD contractor must do today is self-assess against NIST 800-171 requirements, enter the score in SPRS as necessary, and close any remaining gaps. Once these steps have been completed, it is time to begin preparing for additional CMMC practices and the CMMC assessment. Please note that at this time, only companies who have an immediate need to be CMMC certified due to contract requirements will be eligible for certification by CMMC auditors (C3PAOs).

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

In order to receive a CMMC certification, a company must be assessed by a certified C3PAO. An organization may not become certified via self-assessment.