CMMC: A MUST-WIN SITUATION FOR DEFENSE CONTRACTORS

ALCHEMI
ADVISORY GROUP

What you need to know about the Department of Defense's Cybersecurity Maturity Model Certification, why you need to be compliant, and how you need to prepare for an assessment

AN INTRODUCTION TO CMMC

Due to a significant number of breaches by cyber attackers into defense contractors' and subcontractors' information systems, the Department of Defense (DoD) has implemented a new unified cybersecurity standard known as the Cybersecurity Maturity Model Certification (CMMC) in order to protect the sensitive data stored in the databases of its thousands of partners and suppliers in the Defense Industrial Base (DIB).

CMMC uses a maturity assessment framework to outline a series of compliance procedures and processes that are required of organizations in the DIB in order to protect Controlled Unclassified Information (CUI). The origins of that assessment framework lie in the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171.

The DoD has been planning for the implementation of CMMC since January 2020 and preparations have continued unabated in spite of the pandemic. At the start of 2021, the DoD launched CMMC audits for new contracts; the department expects that by 2026, every active contract will require contractors and subcontractors be certified on one of the CMMC's five maturity levels.

DO I HAVE TO PASS A CMMC ASSESSMENT?

In a word. . .YES. Going forward Federal contractors and subcontractors MUST pass a CMMC assessment. If you want to win government contracts, there is no way around it. It is required by the DoD.

Prior to CMMC, organizations were required to be NIST 800-171 compliant, although there was no certification for it; the government relied strictly on an honor system. There were, however, severe penalties if your organization was found to be out of compliance with NIST 800-171—penalties which potentially included losing the government contract.

While keeping the government contract - or winning the contract to begin with - it is a major incentive for companies to be NIST 800-171 and CMMC compliant.

It's is a major incentive for companies to be NIST 800-171 and CMMC compliant.

PLUS, THERE ARE ADDITIONAL BENEFITS:

- Increased Security: The likelihood of a breach declines significantly. In the event that there IS a breach, the impact will be minimized.
- Competitive Advantage: Being compliant gives you a clear competitive advantage over organizations that are not.
- Peace of Mind: Compliance means you can rest easy that your government contract—and your organization's reputation—are safe.

CMMC’S MODEL FRAMEWORK

CMMC’s model framework contains 17 domains, which are comprised of many capabilities.

THE ASSESSMENT IS ORGANIZED BY DOMAINS, NUMBERING SYSTEM AND CAPABILITIES:

Capabilities—CMMC is made up of multiple practices (activities performed at each level) and processes (which delineate the maturity classification for the practices). Each of the processes is assigned to one of five CMMC maturity levels.

Numbering System—The numbering system uses the two-letter domain designation (shown below in parentheses after each domain name), the CMMC level (1 through 5 with 5 being the highest level), and the practice number. For example, the first capability for Level 1 (Establish system access capabilities) is numbered C001 and the first Practice under C001 is to limit information system access to unauthorized users and would be numbered AC.1.001.

Here's How It Works

17 Domains

CMMC’S MODEL FRAMEWORK

Access Control (AC)	• Establish system access • requirementsControl internal system • access Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	◆ Identify and document assets
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	◆ Grant access to authenticated individuals
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	◆ Manage and maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport

CMMC'S MODEL FRAMEWORK CONTINUED

Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	◆ Limit physical access
Recovery (RE)	◆ Manage backups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Assessment (SA)	◆ Implement threat monitoring
System & Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information systems flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections

CMMC LEVELS (Processes & Practices)

The five maturity levels are cumulative, meaning that in order to be certified compliant at a certain level, you must also be compliant at all the lower levels. For example, to be certified compliant at Level 3, you must also be compliant at Levels 1 and 2.

The five levels of CMMC maturity are:

1

Level 1: Basic Cyber Hygiene
Basic safeguarding of FCI (Federal Contract Information)
Practices are performed (at least ad hoc)
0 processes
17 practices

2

Level 2: Intermediate Cyber Hygiene
Transition focuses on protecting CUI
Practices are documented
2 processes
72 practices

3

Level 3: Good Cyber Hygiene
Protecting CUI
Processes are managed (maintained and followed)
3 processes
130 practices

4

Level 4: Proactive
Protecting CUI and reducing risk of APTs
Processes are periodically reviewed, properly resourced, and improved across the organization
4 processes
156 practices

5

Level 5: Advanced/Progressive
Protecting CUI and reducing risk of APT
Continuous improvement across the organization (optimizing)
5 processes
171 practices

SOME FREQUENTLY ASKED QUESTIONS

Before you get started with your pre-audit readiness assessment, here are some things you will want to know.

Is my auditor accredited and independent? You must request and schedule your CMMC assessment to be performed by an accredited and independent CMMC Third-Party Assessment Organization (C3PAO) that is authorized and trained by the CMMC Accreditation Body (AB), a non-profit comprised of experts from industry, academia, and the cybersecurity community.

Which level of certification do I request? When requesting the CMMC assessment for your organization, the level of certification you request will be based on your organization's specific business requirements, which will likely be based on the requirements of the request for information (RFI)/request for proposal (RFP)'s you are seeking.

Who decides which level is best? Ultimately, the government will determine which CMMC level is the best fit for their contracts.

What determines the level of certification my organization will receive? Not all DoD contractors and suppliers handle the same type of sensitive government information. The assessor and CMMC AB will designate the appropriate CMMC certification level based on the proper capabilities and organization maturity your organization demonstrates.

THE ASSESSMENT PROCESS

Companies will want to ensure they are properly prepared before starting an audit with a 3CPAO assessor firm. Although some companies may have the knowledge and technical skills in house to prepare for a CMMC audit the majority will need to seek outside help to ensure they are addressing all of the particulars of CMMC.

This Readiness Assessment phase is crucial to evaluate your overall preparedness and to assist in identifying and remediating those areas where you may be weak.
It will take some patience to get through the pre-audit readiness assessment of your organization.

Each of the following phases of the assessment process takes approximatelythree to four weeks to complete:

- Review business processes
- Technical assessment of systems and networks
- Data analysis

Just a few of the items your CMMC assessment package should include:

- Risk analysis of your cyber environment of the most recent vulnerability scan and penetration testing
- An inventory of your systems to find out how and where FCI and CUI data is stored and how access to information is controlled to find out your present needs.
- A detailed review of each CMMC practice against your environment. The review should include text response and evidence such as screenshots, logs, reports or other evidence.
- Copies of policies and procedures.

Be sure to check your package against the Assessment Guide which was published by the **DoD in December 2020**. Review the assessment objectives and the assessment considerations sections for each practice to make sure that your implementation meets the requirements of the certification level you are trying to achieve.

REQUEST A CONSULTATION TODAY

With your government contract at stake, you will want to know where your organization stands on CMMC compliance before the assessment begins. Your organization may not have the resources to conduct the review of each CMMC practice or perform the pre-audit readiness assessment. You don't want to hear that you are not compliant from an auditor.

A cybersecurity consulting firm such as Alchemi Advisory Group can conduct that readiness assessment for you to let you know where you are compliant and where you need to be - so that the auditor doesn't have to.

If you need a pre-CMMC audit readiness assessment contact Alchemi Advisory Group to request a consultation today via:

888.590.1618
info@thealchemigroup.com
TheAlchemiGroup.com

ALCHEMI
ADVISORY GROUP