TalPoint

CMMC 2.0 Compliance Demystified

Discover the upcoming CMMC changes with its new version and how to prepare for its compliance

www.TalPoint.com

Table of Contents

Introduction

The cyber supply chain is increasingly becoming the weakest link in the cybersecurity infrastructure of defense contractors. Third parties and business associates, such as Cloud Service Providers (CSPs) that work as defense contractors, have long battled to create a reliable cyber defense for sensitive data processed on behalf of their clients.

The US Department of Defense (DoD) created the Cybersecurity Maturity Model Certification (CMMC 1.0) framework in 2020 to help with this and to assure cyber resilience in its supply chain.

The CMMC framework is intended to assist Defense Industrial Base (DIB) contractors in better assessing and improving their cyber security posture by ensuring that all DoD contractors implement cyber security best practices to safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

On July 17, 2021, the DoD announced the introduction of the CMMC 2.0, which would replace the current CMMC certification levels.

The most recent CMMC 2.0 features a few significant modifications that will ease some of the rigorous restrictions imposed by the prior model. The aim for CMMC, however, remains the same: to establish fundamental cyber hygiene requirements to protect sensitive data and create national cyber resilience.

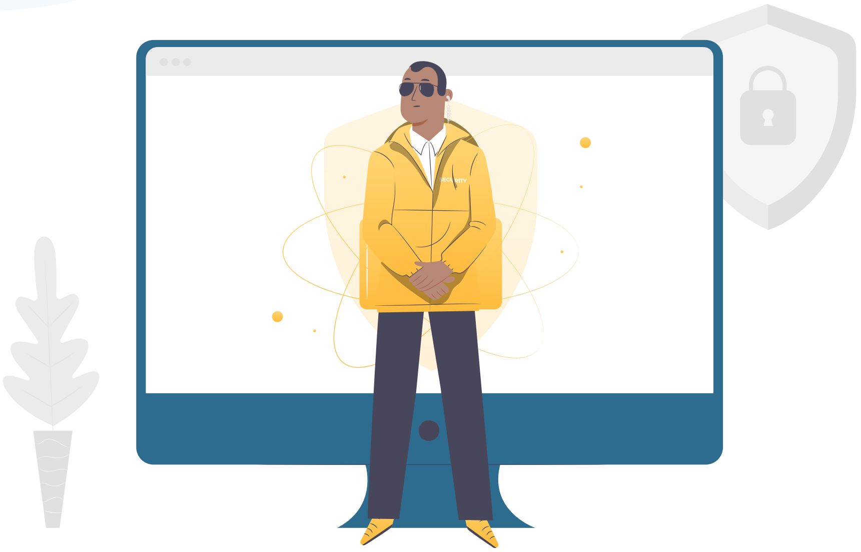
This guide introduces the CMMC 2.0 model, the new levels of CMMC, and how to prepare for your CMMC compliance journey.

Overview of CMMC 2.0

The Cybersecurity Maturity Model Certification, developed in response to the increasing cyber threat scenario, is an overarching standard for cybersecurity implementation throughout the Defense Industrial Base (DIB) and government contractors.

CMMC is also backed by federal universities and institutions, cybersecurity contractors, subject matter experts, and R&D facilities around the country. Its primary purpose is to raise and standardize cybersecurity standards throughout the US DoD supply chain and prevent cybercriminals from gaining access to high-value organizations via weaker linkages in the supply chain.

CMMC compels DoD contractors to undertake external security audits in addition to incorporating all well-known government cybersecurity standards such as the National Institute of Standards and Technology 800-171 (NIST 800-171), NIST SP 800-53, the International Organization for Standardization (ISO) 27001, ISO 27032, and Aerospace Industries Association (AIA) NAS9933.



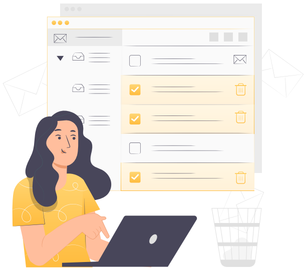
What Has Changed Under CMMC 2.0

The following are the most significant modifications to CMMC:

No More Transition Levels

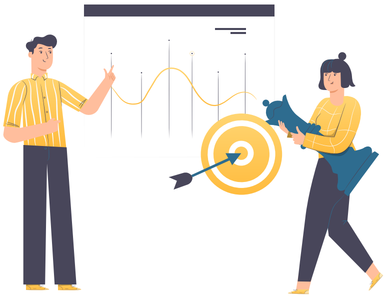
No Third-Party Assessments For Level

Some Level 2 Companies Will Not Require Third-Party Certification



No More Extra Practices

No More Maturity Processes



Plan of Action and Milestones (PoAM)

No More Transition Levels

CMMC 1.0 had five levels of maturity. CMMC 2.0 eliminates the transition levels (Levels 2 and 4), resulting in a simpler model with only three levels.

For firms that do not handle Controlled Unclassified Information (CUI) but solely Federal Contract Information (FCI), CMMC 2.0 Level 1 (Foundational) remains the required level.

The original CMMC Level 3 has been replaced by CMMC 2.0 Level 2 (Advanced). This is the minimum requirement for contractors who work with CUI. However, it only covers 110 of the original Level 3's 130 practices.

The more demanding standards of the original Level 5 are now included in CMMC 2.0 Level 3 (Expert). A small number of contractors will require this sophisticated degree of cybersecurity.

There Will Be No Third-Party Assessments For Level 1

Every maturity level in the original edition of CMMC requires an official evaluation by a Certified Third Party Assessment Organization (C3PAO).

However, businesses now at CMMC Level 1 will no longer be required to undergo such an examination. Instead, they will do an annual self-assessment with senior leadership approval and submit it to the Supplier Performance Risk System (SPRS). As a result, small contractors will save a lot of money on assessment fees.

Some Level 2 Companies Will Not Require Third-Party Certification

This is the most ambiguous change. The Department of Defense has proposed a "bifurcation" of the original CMMC Level 3 standards, prioritizing some acquisitions for third-party evaluation while allowing others to self-attest.

Despite the initial plan to branch out the requirements for Level 2 companies, it appears that the Department of Defense will drop this feature and require all Level 2 companies to be assessed by a Third-Party, according to DoD Deputy CIO David McKeown:

“At level two, this is where we started having controlled unclassified information,” McKeown said on February 10. “We thought maybe we could bifurcate this into the types of QE (qualified entities) that were really important to the department and the ones that were not. But in the end, when we did the analysis, it looks like a universe of about 80,000 companies that are going to fall into this bucket here. Probably all of them will have to get a level two assessment.”

What that means for your organization remains to be seen until more clarification is released. In the interim, it's prudent to plan as though all CMMC Level 2 (previously Level 3) firms will need a third-party evaluation.

No More Extra Practices

This has a direct impact on contractors that handle CUI. The initial CMMC requirements added 20 more practices to the NIST SP 800-171's original 110. These 20 additional criteria have now been eliminated.

No More Maturity Processes

CMMC 2.0 no longer includes the prior version's maturity processes. This significantly reduces the amount of documentation necessary and eliminates most of the uncertainty in the previous paradigm

Plan of Action and Milestones (PoAM)

The old edition of CMMC needed a perfect score. However, like previous Defense Federal Acquisition Regulation Supplement (DFARS) mandates, contractors may now submit a time-bound "Plan of Action and Milestones" to address specific areas of noncompliance.

This implies that a perfect compliance score is no longer required to gain certification. Instead, you can give a specific, time-bound strategy to remedy any gaps in your compliance. You will be reassessed after a period designated by the DoD to ensure the PoAM issues have been fixed.

CMMC 2.0 Compliance Levels

CMMC certifications now fall under one of three levels associated with the National Institute of Standards and Technology (NIST) cybersecurity framework, rather than the five compliance levels described in CMMC 1.0:

Level 1: Foundational ★

Level 1 assessment requirements dictate that companies adopt fundamental measures to prevent cyberattacks. They may, however, be able to implement these activities ad hoc without depending on paperwork and are permitted to achieve certification through an annual self-assessment.

As a result, C3PAOs do not measure level 1 process maturity. Because activities at this level are primarily concerned with the protection of FCI, level 1 only contains practices that fulfill the fundamental safeguarding standards outlined in Title 48 of the Federal Acquisition Regulations (CFR)

Who needs CMMC level 1?

Contractors and subcontractors for the Department of Defense who handle Federal Contract Information (FCI)

Level 2: Advanced ★★

Level 2 mandates businesses describe their processes to steer their efforts toward CMMC Level 2 maturity. This documentation must also make it possible for users to replicate these processes.

Level 2 procedures are defined as advanced cyber hygiene practices (sometimes known as intermediate cyber hygiene) and are a step up from level 1. Level 2 compliance assessment standards vary depending on whether the CUI data handled is essential or non-essential to national security.

For example, organizations with prioritized acquisitions that address vital national security data must undergo a higher-level third-party assessment with a C3PAO every three years. In contrast, non-prioritized assets with non-critical national security data must complete an annual self-evaluation.

Who needs CMMC level 2?

Level 2 compliance is required for DoD contractors and subcontractors that handle the same sort of Controlled Unclassified Information (CUI). The subcontractor may be subject to a lesser CMMC level if the prime merely passes down specific information.

Level 3: Expert ★★★

The level 3 CMMC model decreases a system's vulnerability to Advanced Persistent Threats (APTs) by compelling an organization to develop, implement, and finance a strategy to manage the activities required to implement its cyber security practices.

This plan may include information on various subjects, such as objectives, missions, projects, resourcing, training, and the participation of organizational stakeholders.

This level's cybersecurity measures are solid cyber hygiene procedures that focus on protecting CUI. However, they include the security standards specified in NIST SP 800-171 and the additional 20 practices for CMMC level 2.

DFARS 252.204-7012 remains in effect, imposing additional duties beyond NIST SP 800-171, such as reporting security incidents.

Although the DoD is presently establishing its security criteria, it is akin to CMMC 1.02 Level 5. However, it has already been stated that the Level 3 standards would be based on NIST SP 800-171's 110 controls and a portion of NIST SP 800-172 controls.

Who needs CMMC level 3?

Companies that manage CUI for DoD programs with the highest priority are subject to CMMC 2.0 Level 3.

CMMC 2.0 Implementation and Auditing

The CMMC ecosystem is constantly changing and includes many moving elements. Depending on the CMMC level your firm must attain, you must demonstrate CMMC compliance through self-assessment or be examined and certified by a third-party organization or DoD authorities.

Only a few organizations must certify their compliance through a third-party organization, specifically CMMC level 3 and some level 2 companies.

The US Department of Defense has designated the CMMC Accreditation Body (CMMC-AB) to be the single official source for the successful implementation of CMMC Assessments and Training with the DOD contractor community. This organization changed its name to The Cyber AB in June 2022.

There are two types of organizations you may face on your path to certification. The Cyber AB has trained and registered/certified both of them:

1

CMMC Registered Practitioner Organizations (CMMC-RPO)

Focus on consulting and assisting with all processes leading up to certification testing. This involves a preliminary CMMC gap analysis, repair, installation of missing controls, documentation development, etc. A CMMC Pre-Assessment is advised before the certification audit by a C3PAO.

2

CMMC Third Party Assessor Organizations (C3PAO)

Are primarily concerned with the CMMC Assessment (Certification Audit). They will report their findings to The Cyber AB, who will certify you if relevant. While C3PAOs can offer all of the services that CMMC-RPOs do, they cannot deliver them to the organization they are assessing. This would be a conflict of interest.

The CMMC Certification Process

Each organization, scope, implementation, and certification is unique since it is determined by several elements such as timeframe and cost. Among the most critical factors are the following:

- **Required CMMC Level**
- **DoD contractor's existing infrastructure and cybersecurity posture**
- **The scope of your implementation**
- **The C3PAO's availability to execute the certification assessment**

While these considerations affect timing, the typical example of the CMMC implementation timetable and the CMMC certification procedure below will give you a fair picture of the required stages and some time estimates.

CMMC Gap Analysis

In this phase, you will determine the company goal and analyze the current state vs. the requirements.

Among the items considered are the following:

- Internal Structure
- Processes and controls
- Documentation
- Physical Protection

Implementation

This phase typically takes 6-8 weeks (CMMC Level 1) to 6-12 months (CMMC Level 2), mainly relying on the company and its current information security posture. Implementation of CMMC Level 3 will take at least 12 months.

This includes the following:

- Creating missing documentation
- Putting in place the necessary controls
- Risk identification and management
- Closing gaps discovered during the analysis step.

Observation / State of Readiness

The CMMC Levels after 1 need proof of system maturity. Therefore, you will need time after the implementation phase to create the proper Certified 3rd Party Organization (C3POA) of your choice to conduct the Certification Assessment.

This phase is also utilized to make necessary modifications and enhance procedures.

Certification Assessment

A Certified 3rd Party Organization (C3POA) of your choice will conduct the Certification Assessment.

The complete assessment procedure will take 6-8 weeks and will be divided into three steps:

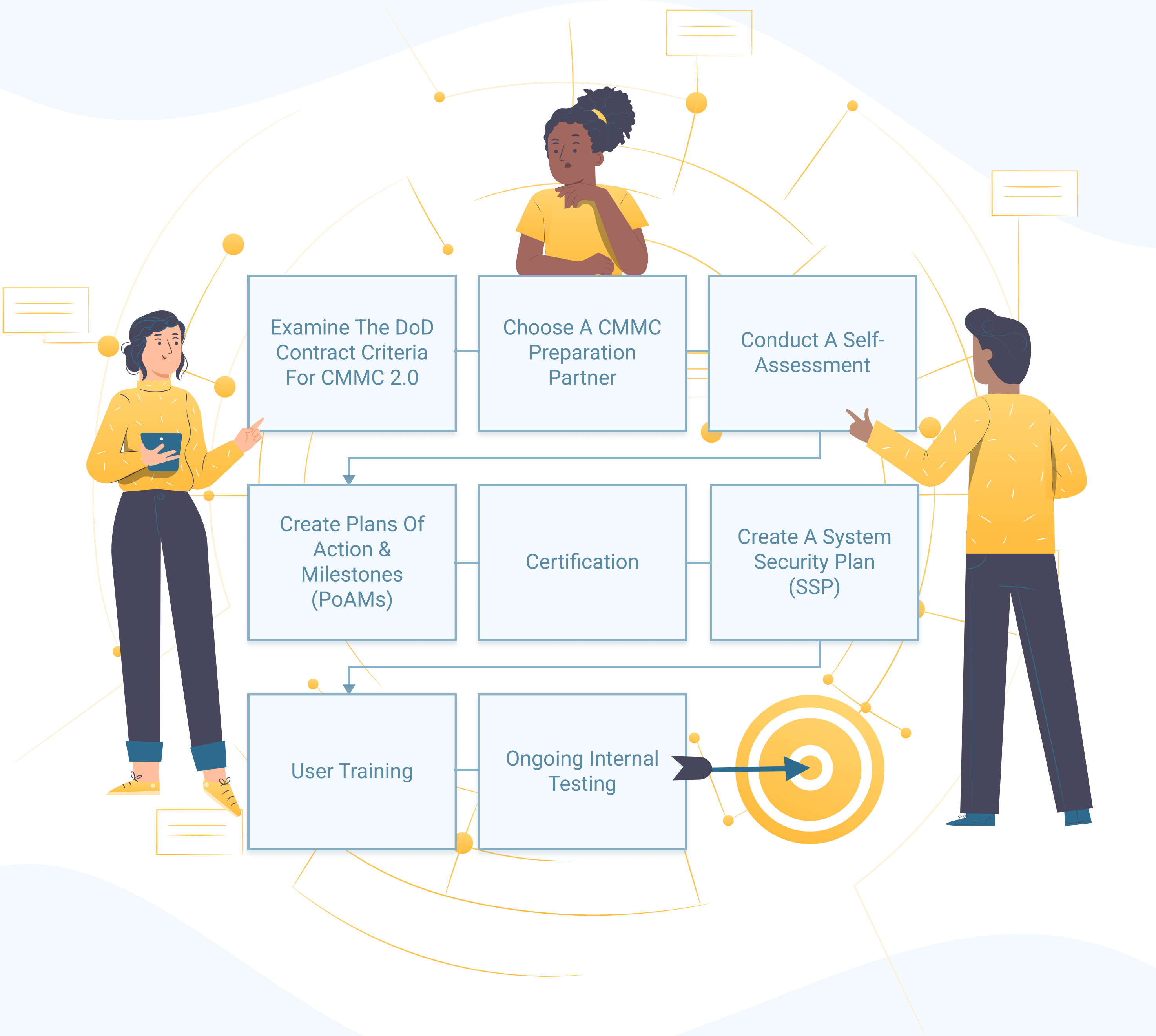
- **Readiness:** The C3PAO will request and review your paperwork.
- **The Assessment:** The C3PAO will visit many on-site days to examine the precise controls and evidence.
- **Reporting Phase:** It will take the C3PAO two weeks to produce the report.

The C3PAO will submit its results to the Cyber AB (previously the CMMC Accreditation Body), which will offer you accreditation.

This phase does not apply to you if you only have CMMC Level 1 requirement or if you fall into the subset of Level 2 that does not contain information necessary to national security.

Preparing for CMMC 2.0

Consider the following strategy for achieving CMMC compliance.



Examine The DoD Contract Criteria For CMMC 2.0

Choose A CMMC Preparation Partner

Conduct A Self-Assessment

Create A System Security Plan (SSP)

Certification

Create Plans Of Action & Milestones (PoAMs)

User Training

Ongoing Internal Testing

STEP 1

Examine the DoD Contract Criteria for CMMC 2.0

Verify the projected maturity level and validate your audit requirements. Determine major compliance deadlines and begin your program immediately.

Confirm your maturity level and audit criteria with the procurement office, and look for updated contract material that confirms your requirements.

STEP 2

Choose a CMMC Preparation Partner

TalPoint experts can walk you through every facet of the CMMC program lifecycle. This involves identifying needs, developing implementation standards, creating controls, preparing for audits, and more. With the right expertise in your back pocket, you can substantially lower risk of non-compliance while meeting your compliance deadlines.

STEP 3

Conduct a Self-Assessment

Depending on your level, this will range from a subset of NIST SP 800-171 to the NIST SP 800-171 110+ practices. The Department of Defense intends to provide fundamental requirements by May 2023; however, you should immediately start because the program will include urgent implementation needs.

STEP 4

Create a System Security Plan (SSP)

This strategy serves as the foundation for NIST SP 800-171 compliance. The SSP can be integrated into your existing cybersecurity initiatives, but it must meet all your levels 1-3 standards.

STEP 5

Create Plans of Action & Milestones (PoAMs)

This document explains why you cannot meet standards, the activities you are doing to resolve the weaknesses, and the plan implementation dates.

STEP 6

Certification

If your contract specifies audit requirements, contact a certifying body early in the development of your CMMC program. Due to the scarcity of certified auditors, audits must be scheduled months in advance. We propose establishing a connection immediately to ensure that the scope, timeframe, and program expenses are all well-defined.

STEP 7

User Training

It is not enough to develop a program; all users must be educated on new CMMC cybersecurity and workflow standards. Instead of hour-long yearly classes that result in minimal retention, try a drip program that includes monthly micro lessons. Make a role-based program that focuses on interacting with CMMC-classified data.

STEP 8

Ongoing Internal Testing

Organizations that are not subject to external audits should develop a self-evaluation procedure. A successful self-assessment program considers all SSP criteria and then assesses the items regularly. The frequency and depth of testing are determined by risk and compliance requirements.

Let TalPoint’s CMMC Experts Support Your Compliance Goals

By partnering with TalPoint, you gain access to our private network of leading cybersecurity experts that can help you assess the unique needs of your organization and execute a comprehensive compliance certification program.

Our compliance and cybersecurity experts can also assist with your self-assessment, if required, and submission to SPRS; and help your company in preparation for your third-party certification audit, if required.

Get Started With TalPoint