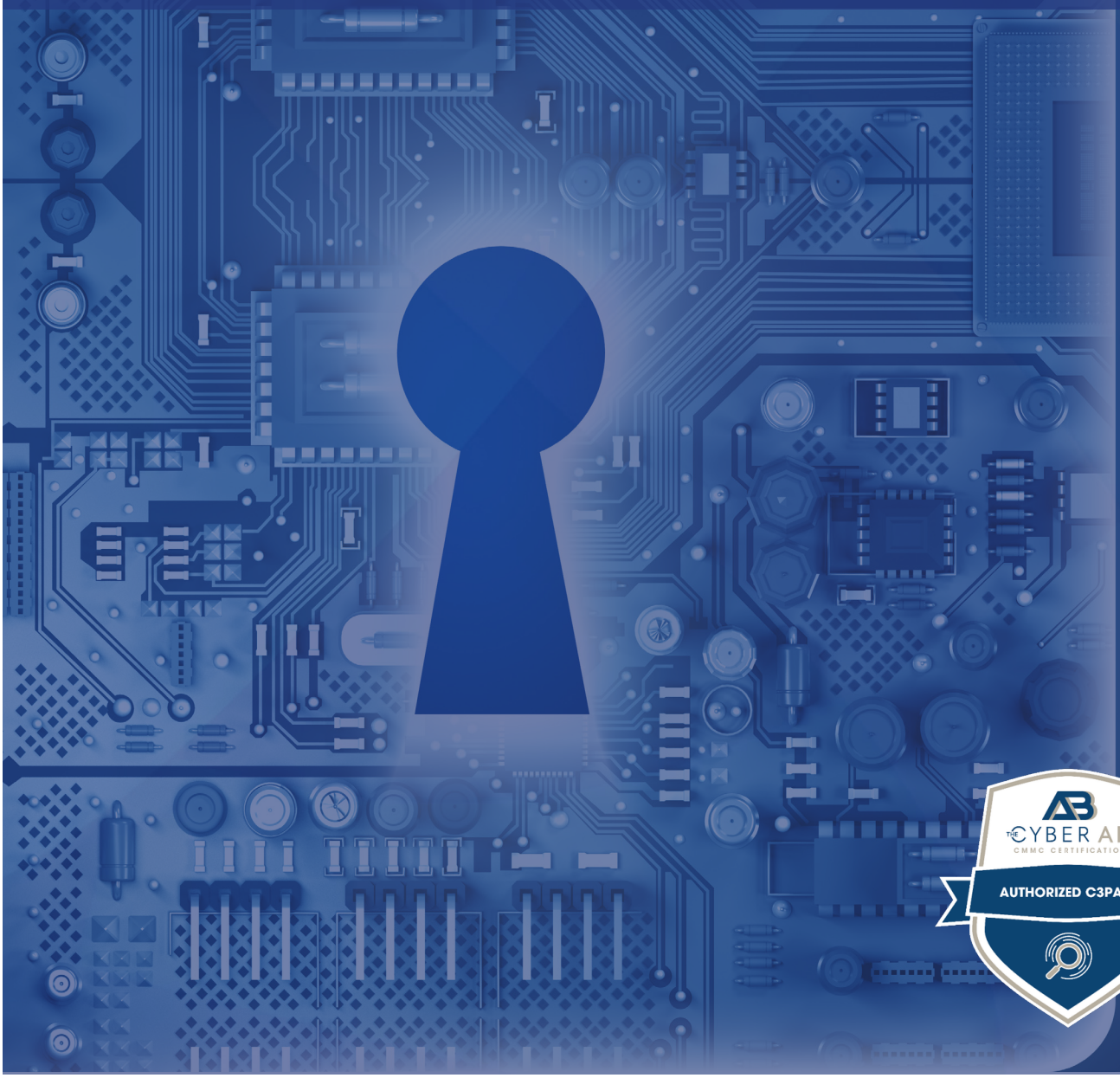
SCHNEIDER DOWNS

Big Thinking. Personal Focus.

CMMC: Cybersecurity Maturity Model Certification Guide



THE CYBER AB

CMMC CERTIFICATION

AUTHORIZED C3PAO

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Cybersecurity Maturity Model

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a Department of Defense (DoD) certification process that measures a Defense Industrial Base (DIB) sector company's ability to protect Federal Contract Information (FCI) and Controlled Classified Information (CUI). Designed as a cybersecurity requirement for all companies that have access to the DoD in any form, the effort shows how the DoD plans to address cybersecurity risk throughout the defense supply chain to protect defense systems and FCI and CUI. The release of the final edition of CMMC Version 2.0 was announced November 2021. Documentation can be found at **DoDCIO.Defense.gov**.

CMMC is designed as a methodology and framework that will constantly evolve as technology changes. Developers intend the certification to be a tool for organizations to improve their cybersecurity practices, but the DoD doesn't want it to become just another compliance checklist. The defense industry is a regular target of state and rogue threat actors attempting to obtain sensitive security data. CMMC is meant to help reduce risk resulting from these cyber threats.

One of the goals of CMMC is to create a unified DoD cybersecurity standard. The CMMC model 2.0 will require organizations to be assessed by a CMMC Third Party Assessment Organization (C3PAO) and the increased competition between C3PAOs will reduce assessment costs for Organizations seeking certification (OSCs). In certain circumstances, OSCs will also have the flexibility to create a Plan of Action & Milestone (PoA&M) in order to achieve CMMC certification.

CMMC Domains

CMMC is based off of the National Institute of Standards and Technology (NIST) SP 800-171 14 families and the Federal Acquisition Regulation (FAR) 52.204-21 requirements. They're listed below for quick reference.

- Access Control (AC)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IDA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PP)
- Risk Assessment (RA)
- Security Assessment (CA)
- System and Communication (SC)
- System and Information Integrity (SI)

Levels of CMMC

There will be three levels of certification within CMMC, each with defined practices and processes that are cumulative and carry into the subsequent level. For example, to achieve Level 3, an organization must meet the practices and processes for CMMC Level 1, 2 and 3. Full definitions of level requirements are provided below:

Level 1 | Level 1 is the "foundational" level of CMMC compliance requires all contractors that have FCI in their contracts to implement a set of 17 basic cybersecurity practices that are required by the FAR 52.204-21. Organizations that fall under level one may perform an annual self-assessment of the FAR 52.204-21 controls and report there score to the Department of Defense.

Level 2 | is the “advanced” level of CMMC that requires contractors that handle CUI to implement the NIST 800-171 framework which includes 110 practices from 14 CMMC families. If a contractor handles sensitive CUI, the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 requires the contractor to be level 2 certified by having a C3PAO perform an independent assessment to validate that the contractor has fully implemented the NIST 800-171 framework.

Level 3 | is the “expert” level of CMMC maturity that is required for contractors that work with critical DoD infrastructure. Organizations seeking level 3 certification will be required to comply with the NIST 800-172 framework. Level 3 contractors are also required to be accessed by the DoD directly as opposed to an independent C3PAO. Organizations will need to become certified for level 2 practices by a C3PAO prior to being assessed by the DoD for level 3.

Who Does CMMC Affect?

Starting in 2025, all companies that conduct business with the DoD and suppliers across the DIB will need to acquire some level of CMMC certification. This means that every prime contractor and subcontractor of the DoD will have to be audited and certified under the CMMC framework. The DoD expects CMMC to take five years to fully roll out and not really get going until 2026. This will affect more than 300,000 organizations, including entities in the U.S and their international partners. The level of certification (1-3) that each company needs to attain will depend on the amount of FCI or CUI it processes. Unless a higher level is specified, all contractors and subcontractors must meet a minimum of CMMC Level 1. The government and DoD will determine the appropriate tier requirement for contracts they administer. The required CMMC level will be documented within the appropriate Request for Proposal (RFP).

How Do I Get Certified?

The Defense Industry Base Cybersecurity Assessment Center (DIBCAC) will allow organizations that are required to comply with CMMC level 1 to complete a self-assessment. Organizations that are required to comply with levels 2 and 3 are required to be assessed by a third-party and the DIBCAC. Independent assessments of CMMC will be completed by C3PAOs. The **Cyber AB** recently created not-for-profit independent group of stakeholders, is charged with training, and certifying the third-party assessors. C3PAOs will evaluate organizations to determine if appropriate capabilities and organizational maturity, as well as proper controls and processes, are in place to reduce the risk of specific cyber threats.

How Will the Scope for a CMMC Assessment Be Determined?

As part of the planning and preparation process of a CMMC assessment, a OSC will need to self-identify the assessment scope that is based on the environment where FCI and/or CUI is processed, stored, and transmitted and provide the scope to the C3PAO performing the assessment. The C3PAO will request and review the asset inventory, System Security Plan (SSP) and network diagrams to verify that the identified scope is consistent with where FCI/CUI is process, stored and transmitted. The scope of an assessment may also be scoped within an enclave, which is a segmented portion of the network or data that is protected by a security perimeter to prevent FCI/CUI from leaving the enclave. This may help OSCs reduce security costs by only applying certain CMMC security controls to the enclaved environment. If an OSC uses a Third-Party service provider (TSP) for cloud-hosting services and the TSP stores FCI/CUI, the OSC will need to ensure that the TSP has achieved a current FedRAMP moderate or higher certification. If a TSP is not FedRAMP certified, the current expectation is that the TSP will need to achieve a CMMC Level 2 certification.

What Are the Associated Costs of CMMC?

While there is not a determined fixed cost for becoming CMMC certified, the cost of becoming certified will be dependent on an organizations environment, size, and the number of assets. OSCs will likely need to implement additional resources, assets and controls in order to become compliant with the CMMC levels and the cost of those will be dependent on the size of the OSCs environment. Additionally, OSCs that need to be level 2 certified will need to hire a C3PAO to conduct the assessment and the cost of doing business with the C3PAO will be dependent on several factors including resources, assets, environments (on-premise vs cloud), location, etc. Additionally, OSCs may want to consider hiring a C3PAO (that is different then the C3PAO conducting the assessment) to complete a readiness review assessment to avoid findings during the real assessment that will need to be remediated quickly. It is still unknown if there will be a cost for receiving a DoD assessment for OSCs that will need to be level 3 compliant.

What Are the Next Steps and What Can You Do to Prepare for CMMC?

The Cyber AB is developing the oversight and requirements of the certifier accreditation program, along with working to train and certify the C3PAOs. CMMC requirements are expected to be included in select Requests for Information (RFIs) in Q1 2025 and RFPs. While CMMC certification may not be required for all DIB organizations immediately, implementing CMMC requirements and practices will require an investment of time and money. There are several things to do now to start preparing for CMMC:

Determine when the period for current contracts ends and when contract re-competes will occur

CMMC will change the entire acquisition process for DoD contracts, coming into effect when bidding on new contracts or when current ones are up for re-compete. It's expected to take up to five years to fully roll out. Any company currently working with the DoD will need to be certified (at Level 1 at the minimum) at some point over the next five years if they want to continue working with the department. Companies should be working to meet the appropriate level of CMMC prior to the date of their contract re-compete, or whenever they plan to bid on new contracts, as they will be required to meet that certification level at time of award.

Review the current documentation for CMMC Version 2.0

CMMC Version 2.0, officially released November 2021, includes a few changes from the 1.0 version released in January 2020. Documentation contains the CMMC model and provides detailed descriptions of each level, the domains and capabilities, and process maturity. There are also instructions on how to read and use the model. The full draft model and a description of practices that should be in place for each level are documented as Appendix A. The model maps practices to NIST SP 800-171 controls and other existing standards. The Version 2.0 document also includes discussion and clarification with examples for practices in Levels 1-3.

Determine what level of business your company wants to do with the DoD

The level of CMMC that each company will need to meet depends on the type of business the organization is doing with the DoD, and correlates to the type of data it will access. For example, if an organization is working or plans to work under DoD contracts that involve CUI, it will be required to meet at least Level 2 practices and processes maturity. Organizations will need to implement a strategy to meet CMMC practice and process maturity requirements for the appropriate level to continue work on DoD projects.

Identify areas where there may be gaps with CMMC

In reviewing CMMC documentation, determine if your organization has any gaps in processes or practices for your desired level of certification. These will be areas to invest in and improve as soon as possible. If your company has completed any other self-assessment, compliance audits or certifications (NIST SP 800-171, 800-53, ISO, SOC2, etc.), that's a great place to start identifying gaps or deficiencies. If any are noted that map to CMMC practices, begin to work on resolving items based on priority.

If your organization has completed a self-assessment for NIST SP 800-171, you may have developed and documented a Plan of Actions and Milestones (POAM) for any controls that have not been met. For CMMC, however, you'll need more than

just a plan or POAM to meet certification requirements. In order to achieve a certain level, all practices for that level must be met. You'll want to close as many gaps as possible for your desired level of certification in order to continue doing business with the DoD and improve your chances of winning new DoD contracts.

Review your supply chain for any risks

For primes on a contract, any subcontractors used may also need to meet a certain level of CMMC. This should be specified in the DoD contracts. It is the prime's responsibility to make sure requirements are being met by any subcontractors being utilized to complete DoD work. To prepare for CMMC, contactors should be communicating to business partners and suppliers to ensure they're aware of the upcoming requirements.

CMMC implementation is a corporate business issue, not just an IT concern. To continue to do business with the DoD, DIB organizations will eventually have to meet CMMC requirements. The certification will take at least five years for the process to fully implement, as current contracts start to expire over that timeframe. This will be a big transition, but the government plans to work closely with companies and incorporate feedback as it starts the certification process and awards contracts with the new requirements.

The DoD recognizes the need for the defense industry to have continuous security principles incorporated into its work and throughout the supply chain. CMMC represents a major step toward improving cybersecurity hygiene throughout all levels of the DIB and reducing risk to defense agencies' systems and sensitive data.

How Schneider Downs Can Help

Schneider Downs is one of the first 55 authorized C3PAOs in the nation. We can help your organization become CMMC certified by conducting an official CMMC assessment against your organization. Schneider Downs has several CMMC Certified Professionals (CCP) and CMMC Certified Assessors (CCA) who are trained in using the CMMC Assessment Process (CAP). Schneider Downs is also able to help with a readiness consulting engagement to identify gaps within your controls and help remediate those gaps prior to your CMMC assessment.

For more information, please contact our team at **contactsd@schneiderdowns.com** or visit **www.schneiderdowns.com/cmmc**.

About Schneider Downs IT Risk Advisory

Schneider Downs' team of experienced risk advisory professionals focuses on collaborating with your organization to identify and effectively mitigate risks. Our goal is to understand not only the risks related to potential loss to the organization but to drive solutions that add value to your organization and advise on opportunities to ensure minimal disruption to your business.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX
AUDIT AND ASSURANCE
CONSULTING
WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

METROPOLITAN WASHINGTON
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003