[A Beginner's Guide to Getting CMMC Certified | 38North Security](https://38northsecurity.com/article/how-do-i-get-cmmc-certified-a-step-by-step-walkthrough-for-beginners/)

So you’ve reviewed your contracts and determined that you have a requirement to protect Federal Contract Information ([FCI](https://www.acquisition.gov/far/52.204-21)) or Controlled Unclassified Information ([CUI](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF)), and you’re wondering how to get Cybersecurity Maturity Model Certification ([CMMC](https://38northsecurity.com/security-compliance/north-america/cmmc/)) certification for your business. You’ve come to the right place. We’re going to ease into the basics of CMMC compliance to get you ready for the complex process ahead.

The CMMC is a critical standard for companies working with the U.S. Department of Defense. This article will walk you through the high-level concepts you need to understand, the different CMMC levels and requirements to prepare your documentation, selecting an assessor, and managing the costs associated with the process.

After reading this guide, you’ll be ready to tackle the more detailed and nuanced next steps to CMMC compliance.

[*Start here for your CMMC certification process.*](https://38northsecurity.com/security-compliance/north-america/cmmc/)

**Key Takeaways**

* The CMMC program is designed to enhance the defense supply chain integrity by requiring companies working with the DoD to undergo rigorous assessments and meet specific security standards at different levels.
* Organizations must identify their required CMMC level based on the information they handle, perform a gap analysis, develop a System Security Plan (SSP), and be prepared for costs that vary with business size and cyber readiness before undergoing formal assessments by Certified Third-Party Assessment Organizations (C3PAO).
* CMMC 2.0 simplifies the previous model by consolidating from 5 to 3 levels, aligning with National Institute of Standards and Technology (NIST) standards, and allows for self-assessments and government waivers in certain conditions, emphasizing ongoing compliance through continuous monitoring, regular updates, and recertification.

*Looking to Achieve CMMC Certification?*[*Get in touch with a cybersecurity expert*](https://38northsecurity.com/contact/)*today.*

**Understanding the CMMC Certification Path**

[CMMC](https://38northsecurity.com/article/what-is-cmmc-compliance-a-brief-intro-for-csps-exploring-certification/), short for Cybersecurity Maturity Model Certification, is a certification that combines various cybersecurity standards and best practices under one unified framework. Now known as CMMC 2.0, the program aims to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) from cyber threats, thereby enhancing the integrity of defense supply chains.

Companies aiming to acquire DoD contracts or be part of the Defense Industrial Base can only do so by achieving CMMC compliance first. The certification process is rigorous and thorough, designed to ensure compliance only from those who exhibit robust cybersecurity practices.

*Learn more:*[*What is CMMC Compliance? A Brief Intro for CSPs Exploring Certification*](https://38northsecurity.com/article/what-is-cmmc-compliance-a-brief-intro-for-csps-exploring-certification/)

**Deciphering CMMC Compliance Levels**

CMMC has three compliance levels. Each level represents a step up in the maturity and robustness of a company’s cybersecurity practices:

1. Level 1 Foundational: Focuses on the protection of FCI
2. Level 2 Advanced: Focuses on the protection of CUI
3. Level 3 Expert: Focuses on the protection of CUI from Advanced Persistent Threats (APTs)

Each level of CMMC compliance has its requirements and assessment procedures. Level 1 requires organizations to meet the requirements of 17 cybersecurity practices from the Federal Acquisition Requirements (FAR) document 52.204-21 and perform an annual self-assessment. Level 2, on the other hand, requires organizations to implement 110 controls from NIST SP 800-171 rev 2. For most systems, a formal certification for Level 2 involves a third-party assessment every three years. However, a small subset of organizations that do not handle any information critical to national security will be allowed to perform and submit an annual self-assessment. Level 3 requires an organization review and measure practices for effectiveness, as well as implement NIST SP 800-171 rev 2 and a subset of enhanced security practices from NIST SP 800-172 requirements.

**Identifying Your Required CMMC Compliance Level**

Determining the appropriate [CMMC level](https://38northsecurity.com/article/determining-your-compliance-what-cmmc-level-do-i-need-for-my-business/) for your organization is a critical step toward CMMC compliance. This determination is based on the type of information your organization handles. If your organization handles Federal Contract Information (FCI), then you must achieve at least Level 1 certification. If you hold more sensitive Controlled Unclassified Information (CUI), then you must achieve at least Level 2 certification.

Your level of CMMC compliance is also dictated by the sensitivity of the information your organization handles. For example, if your organization deals with critical national security information, you may be required to comply with CMMC Level 3. In addition, it’s vital that your Managed Service Providers (MSPs) or Managed Security Service Providers (MSSPs) also comply with the appropriate CMMC level to protect sensitive information.

*Learn more:*[*What CMMC Level Do I Need for My Business?*](https://38northsecurity.com/article/determining-your-compliance-what-cmmc-level-do-i-need-for-my-business/)

**Preparing for CMMC Certification**

Once you’ve identified the level your organization requires, you must now prepare for the certification process. Preparing for a CMMC assessment necessitates conducting a gap analysis to identify shortfalls in the organization’s security posture and then developing a remediation plan to address these gaps.

Creating and reviewing System Security Plans (SSPs) and Plans of Action and Milestones (POAMs) is another vital component of proving CMMC compliance. Businesses must demonstrate compliance in their operational processes and be vigilant about managing new compliance risks introduced by changes in products, clients, data types, or technologies.

**Conducting a Gap Analysis**

A gap analysis is one of the first steps in preparing for certification. A gap analysis is the evaluation of your organization’s current cybersecurity practices against the certification requirements. This evaluation will help you identify what improvements need to be made to achieve the desired level of CMMC maturity.

A self-assessment is recommended for organizations to pinpoint existing gaps between their security measures and the comprehensive CMMC assessment requirements. Once these gaps are identified, organizations should create a Plan of Action and Milestones (POAM) to outline specific remediation steps for deficiencies. This POAM serves as a critical accountability and improvement tool for the organization’s security posture.

**Developing a System Security Plan (SSP)**

After conducting a gap analysis, the next step is to develop an SSP. The SSP is a critical document that outlines how an organization secures its systems to meet CMMC requirements. At a minimum, it includes information about:

* System boundaries
* Components
* Network configurations
* Access controls
* Connections to other systems
* Contingency procedures
* Incident response plans
* Roles and responsibilities of security team members

The SSP should also document the implementation of security controls, including any existing compliance gaps with Plans of Action & Milestones (POA&Ms). Such documentation plays a pivotal role in demonstrating readiness during CMMC assessments.

*Learn more:*[*Here’s Why a Plan of Action and Milestones (POA&Ms) is Crucial to FedRAMP and CMMC Compliance*](https://38northsecurity.com/article/heres-why-a-plan-of-action-and-milestones-poam-is-crucial-to-fedramp-cmmc-compliance/)

Regular review and timely updates to the SSP are necessary to:

* adapt to changes in the IT environment.
* evolve with newly identified cyber threats.
* keep up with alterations in security controls.
* maintain compliance and effective cybersecurity.

**The CMMC Certification Process**

After gathering CMMC requirements, you must next undergo third-party assessments. This involves sourcing an authorized CMMC Certified Third-Party Assessment Organization (C3PAO) from the Cyber-AB Marketplace website or conducting a self-assessment using CMMC Assessment Guides.

The formal assessment verifies the organization’s SSP, reviews evidence, and interviews personnel to determine CMMC certification eligibility. This can be challenging due to the complexity and rigor of security requirements, and the necessity to continually maintain cybersecurity practices. Organizations should budget at least six months for this process.

**Selecting a Certified CMMC Assessor**

Choosing a C3PAO forms an integral step in the CMMC certification process. When selecting a C3PAO, organizations should confirm the assessor is authorized by the Cybersecurity Maturity Model Certification Accreditation Body (Cyber-AB). Authorized C3PAOs will be officially listed on the Cyber-AB Marketplace.

C3PAOs are responsible for conducting comprehensive assessments of an organization’s cybersecurity practices against the CMMC framework specifically for Level 2 compliance. Hence, verifying that the selected C3PAO has a team with essential cybersecurity expertise for designing and implementing a security program aligned with NIST and CMMC standards is mandatory for organizations.

**Engaging in a Formal Assessment**

A C3PAO reviews security documentation, conducts interviews, and carries out on-site inspections to evaluate an organization’s adherence to CMMC requirements during formal CMMC assessments.

Contractors targeting CMMC Level 2 must demonstrate compliance with NIST SP 800-171 rev 2 by implementing 110 security practices, which are verified during the formal assessment. After completion of the assessment, the C3PAO issues a report which is then submitted to the Cyber-AB for certification, marking the completion of the formal assessment.

**Navigating CMMC Assessment Costs**

CMMC certification costs can vary widely depending on factors such as:

* Business size
* Number of locations
* Existing cybersecurity readiness
* Complexity of the business model, including IT staff size and technology used.

Assessment costs for obtaining CMMC certification, also known as CMMC certification cost, have estimated starting points, with Level 1 assessments beginning at approximately $20,000 and Level 3 certification costs ranging between $3,000 and $100,000.

The cost of a CMMC gap analysis and overall preparation can vary based on organizational size and the current cybersecurity maturity level, which dictates the training and documentation efforts required.

**Maintaining Compliance Post-Certification**

Maintaining compliance post-certification is an ongoing process that requires continuous vigilance and effort. For DIB contractors, annual self-assessments are pivotal in maintaining CMMC compliance, and a full recertification for CMMC Level 2 must be completed by a C3PAO every three years.

Under CMMC 2.0, contractors requiring Level 1, and some Level 2, because they handle non-critical information can conduct self-assessments which streamlines the certification process as compared to the prior mandatory third-party assessments. Contractors must:

* Submit an annual affirmation from a senior company official
* Include their self-assessment results
* Follow the guidelines outlined for Level 1 and some Level 2 requirements
* Submit these to the [Supplier Performance Risk System (SPRS)](https://www.sprs.csd.disa.mil/)

**Leveraging Support Resources**

While achieving and maintaining CMMC compliance may pose challenges, utilizing support resources can significantly simplify this process. The CMMC Level 1 self-assessment guide can be downloaded from the Office of the Secretary of Defense’s website to help organizations prepare for certification.

In addition, a free self-assessment tool provided by the CMMC Information Institute is available to aid in the CMMC Level 1 self-assessment process. The CMMC Accreditation Body (Cyber-AB) also offers CMMC self-assessment guides through official channels to assist contractors in the self-assessment process.

Organizations can also leverage support from a CMMC Registered Provider Organization (RPO) to efficiently achieve and maintain CMMC compliance.

**Ensuring Success with CMMC 2.0**

CMMC 2.0 has been realigned with established standards from the NIST, thus adhering to widely recognized cybersecurity benchmarks. The updated framework emphasizes partnership between the DoD and the private sector to jointly counter evolving cyber threats. Government waivers can be permitted under CMMC 2.0 for specific scenarios, suggesting a level of flexibility in the implementation of cybersecurity requirements.

**Summary**

In conclusion, achieving and maintaining CMMC compliance is a rigorous but necessary process for organizations working with the DoD. It requires a thorough understanding of your organization’s security posture, diligent preparation, and continuous effort to maintain compliance. However, with the right resources, guidance, and commitment, it is an achievable goal that not only ensures compliance but also significantly enhances the security of your organization’s data and systems.

[38North Security](https://38northsecurity.com/) is a CMMC Registered Practitioner Organization (RPO). [Speak to a Cyber-AB RP](https://38northsecurity.com/contact/) today to help you [achieve CMMC certification](https://38northsecurity.com/security-compliance/north-america/cmmc/).

**Frequently Asked Questions**

**What is the Cybersecurity Maturity Model Certification (CMMC)?**

The Cybersecurity Maturity Model Certification (CMMC) is a program developed by the Department of Defense (DoD) to enforce cybersecurity standards for the DoD supply chain and contractors working with the DoD.

**How many levels of certification are there in CMMC?**

There are three levels of certification in CMMC, providing different requirements for organizations based on the sensitivity of the information they handle.

**How much does it cost to get CMMC certified?**

Getting CMMC certified can cost anywhere from $20,000 for a Level 1 assessment to up to $100,000 for Level 3 certification, but choosing an experienced assessor can provide a cost-effective approach.

**How long does it take to get CMMC certification?**

Getting CMMC certification typically takes 12-18 months, as organizations must document and demonstrate the effectiveness of implementing required practices. A CMMC third-party assessment organization will audit and certify these practices.

**Can you self-certify CMMC?**

Self-assessments can be used to meet CMMC Level 1 requirements. In addition, a small subset of contracts with Level 2 requirements but that do not involve information critical to national security will be allowed to conduct self-assessments as under CMMC Level 1. However, the majority of Level 2 and all Level 3 requirements related to national security must be certified by a C3PAO or the DoD.