caetra.io

CMMC Certification: The Definitive Guide

(Licensed from Adobe Stock)

As the initial deadlines for the Cybersecurity Maturity Model Certification (CMMC) approach, many U.S. Department of Defense (DoD) contractors find themselves unprepared to meet compliance. In previous years, DoD contractors were asked to self-certify their compliance with the NIST 800-171 Cybersecurity standards. However, in 2019 the DoD announced a new program known as the Cybersecurity Maturity Model Certification which will require contractors dealing with controlled unclassified information (CUI) to affirmatively prove their compliance with certain elements of NIST SP 800-171 through a third-party assessment.

CMMC aims to protect the Department of Defense supply chain while providing a clear and verifiable way for DoD to verify that contractors have a robust cybersecurity program in place. As nation-state attacks against U.S.-based defense contractors have increased, safeguarding national security with aggressive cybersecurity measures has become all the more important. Once CMMC has been implemented, assessors will audit the cybersecurity program of the companies in question and issue certification that they have achieved compliance with their designated CMMC Level. Let's get a few basics out of the way, then jump into how CMMC can benefit your business and your bottom line.

Who needs to get CMMC certified?

CMMC is a regulation established by the Department of Defense that applies to any government contractor handling controlled unclassified information. CUI is just what it sounds like - information that DoD does not want to be made public, but does not fall under the formal government data classification system. CMMC operates with multiple levels depending on the amount and type of information you are dealing with. Each DoD RFP will specify a level of CMMC certification that you will be required to comply with in order to compete for the award. The levels range from Level 1 (Basic Cyber Hygiene) to Level 5 (Advanced/Progressive).

In addition, CMMC will apply to federal subcontractors that work with the Defense Industrial Base (DIB) prime contractors. They will be required to meet the same CMMC Level as the prime contractor and also require proactive CMMC certification in order for the prime contractor to award them a subcontract.

How will companies get CMMC certification?

The Department of Defense has established a CMMC accreditation body (CMMC-AB) which will authorize third-party assessment organizations (C3PAOs) to act as auditors for CMMC. Assessors will conduct a full audit of each contractor's IT environment and compare it against the cybersecurity practices outlined in the maturity Level that the contractor is aiming to meet. For example, if a contractor is aiming to be certified at CMMC Level One, they must comply with requirements specified in 48 CFR 52.24-21 and NIST SP 800-171, which details 17 basic cyber hygiene practices to protect FCI (Federal Contract Information).

What are the levels of CMMC certification?

CMMC Compliance is broken down into 5 Levels, each level building on the last. For example, Level One contains 17 cybersecurity practices, while Level 2 contains 72 (17 from Level one in addition to 55 additional practices). CMMC practices are drawn from security controls from NIST 800-171, ISO 27001, NIST 800-53, DFARS 252.204-7012, ISO 27032, FedRAMP and a few other sources. Together these controls create the standards of compliance for DoD contractors/subcontractors to follow regarding their internal systems and operations. Depending on the type of work you will be doing, or your subcontractors will be doing, you may want or need to aim for a specific CMMC Level. Read on to learn more about each CMMC compliance level.

- ## CMMC Level 1 Compliance (Basic Cyber Hygiene)

  Level 1 CMMC compliance requires meeting 17 fairly basic security requirements. Many organizations that fall under Level 1 deal with very little CUI and most likely just need to protect Federal Contract Information (FCI). The security requirements include security policies and procedures, access controls, and basic cyber hygiene. Most organizations should already have the elements in place to meet Level 1 CMMC requirements to safeguard existing business information.

- ## CMMC Level 2 Certification (Intermediate Cyber Hygiene)

  CMMC Level 2 requires meeting 72 cybersecurity requirements, expected to establish and document policies for CMMC compliance. These requirements include 48 taken directly from NIST SP 800-171. Level 2 CMMC requirements encompass a wide range of security controls and include access controls, continuous monitoring, awareness and training, and risk management.

- ## CMMC Level 3 Compliance (Good Cyber Hygiene)

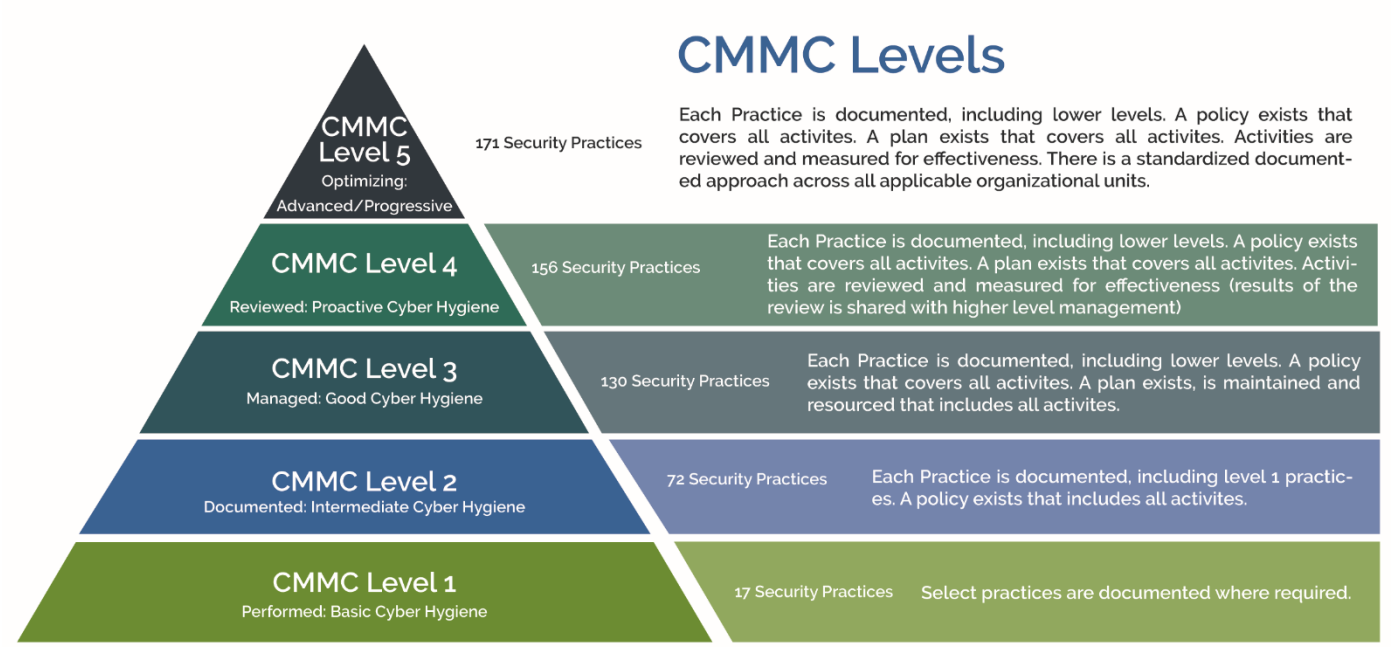
  CMMC Level 3 requires meeting an additional 58 requirements of cybersecurity hygiene practices from NIST SP 800-171 for a total of 130 practices. Level 3 CMMC requirements include demonstrating a basic ability to secure CUI and effective implementation of many controls from NIST SP 800-171. When organizations reach this CMMC Level they should be able to proficiently implement, organize, and maintain security activities while reviewing policies, procedures, and processes with a detailed plan in mind.

- ## CMMC Level 4: Proactive Cyber Hygiene

  CMMC Level 4 requires meeting an additional 26 cyber hygiene practices from NIST SP 800-171B, plus other cybersecurity compliance requirements, for a total of 156 hygiene practices. Contractors looking to meet CMMC Level 4 must demonstrate that they can proficiently defend CUI from advanced persistent threats (APTs) and malicious attacks looking to mine sensitive information. At this Level, DoD contractors and their subcontractors should review and document security activities for effectiveness and inform upper management of any issues that may occur.

- ## CMMC Level 5: Advanced/Progressive

  CMMC Level 5 represents a comprehensive, efficient, and streamlined cybersecurity program that can reduce the risk of both common cyber threats, as well as APTs such as nation-state actors and large criminal organizations. CMMC Level 5 requires the implementation of 171 security practices and closely aligns with the full implementation of NIST 800-171.



What Level of CMMC Certification should my contracting company aim for?

Many organizations may be tempted to seek certification for Level 1 or 2 of CMMC given the ease of implementing a few dozen cybersecurity controls. However, attaining a minimum certification Level of 3 or greater can place your business in a stronger position against another contractor. A large plurality of contracts will likely require Level 3 compliance and attaining these certifications can help your business obtain associated security certifications and DoD contracts.

How to obtain a CMMC Certification

Businesses looking to obtain a CMMC certification must pass an audit from a third-party assessment organization or credited individual assessor. CMMC does not allow businesses to self-certify. The third-party assessment organization or credited individual assessor is known as the C3PAO. The C3PAO are the only organizations authorized to manage and certify assessments for businesses seeking CMMC compliance. C3PAOs can provide many services beyond just the CMMC certification. A C3PAO can offer advisory services to businesses, hire and train other assessors, schedule CMMC assessments, and review CMMC results with the CMMC-Accreditation Body (AB) Quality Auditors.

How can Automating the Compliance Process Help?

If you are a DoD contractor passing certification the first time can save you tens of thousands of dollars. CyMetric simplifies compliance and allows you to easily match IT security controls with compliance requirements and clearly understand gaps in your existing compliance program. An independent review utilizing CyMetric can help catch flaws and vulnerabilities in your security approach that may cause problems on an audit. Preparation is key.

What is the C3PAO audit process?

Before beginning the audit process, businesses seeking CMMC certification should identify the CMMC level they expect to be audited for and the desired maturity level they wish to attain. Next, a business must seek out an authorized C3PAO available to schedule the CMMC assessment with the independent assessor.

When performing the assessment, the independent assessor will evaluate security gaps and vulnerabilities to determine if the business environment meets CMMC requirements needed for that specific level of compliance 1-5. Lower level CMMC certifications will be far easier for many companies to attain than higher level certifications.

What if I fail my CMMC assessment?

After the assessment, businesses will have up to 90 days to resolve any security issues found by the C3PAO and close any gaps necessary to obtain the desired results. If your company seeks an assessment for CMMC Level 3 and fails, you will not automatically obtain CMMC Level 2 certification. You will need to remediate any issues found in your audit and reassess within 90 days. If your business achieves compliance at any level, a CMMC certification notice will be made public knowledge with specific findings from your assessment kept private for security and privacy concerns. If you fail your CMMC certification, it will not be made public.

Do I need to pay for CMMC Certification?

The cost of a CMMC certification is considered an allowable, reimbursable cost by DoD and will be valid for three years after assessment.

What is the value in proactive CMMC Certification?

The CMMC framework represents a multi-front opportunity for DoD contractors. First, CMMC provides a set of clear guidelines for building an effective cybersecurity program that will not only stand up to regulatory scrutiny but can also reduce the risk of your organization suffering a significant data breach. Building a streamlined and coherent cybersecurity program is particularly critical for 2021 and beyond as the rate and complexity of cyberattacks continue to increase.

- **An Impetus to Formalize Your Organization's Cybersecurity Program**

  COVID-19 has caused an explosion in cybercrime which makes building a cybersecurity program all the more critical. By adhering to CMMC Level 3 or greater, you will also be building a comprehensive and streamlined cybersecurity program that enables you to protect your organization more efficiently and at a lower cost than by taking a piecemeal approach. Mid-sized and even small businesses in today's IT environment would do well to take the steps that CMMC Level 3 requires, whether or not they need to go through the CMMC certification process.

- **Competitive Advantage for Companies that Achieve Certification**

  Secondly, many organizations may conclude the effort of compliance is too high, narrowing the pool of companies competing for DoD contracts. This means that meeting Level 3 CMMC compliance could easily allow you to competitively bid on contracts that may have been previously out of reach. According to Peter Clay, the former CISO of Deloitte's Federal Practice:

  "CMMC represents an opportunity for DoD contractors to both formalize their cybersecurity program while making themselves more competitive on previously unattainable contracts."

  In addition, a CMMC Level 3 or greater certification can serve as a mark of trust not just for DoD but for other lines of business. Large enterprises and other government agencies are becoming increasingly concerned about supply chain security. Being able to show that you have developed a compliant, comprehensive, and DoD approved cybersecurity program can make the difference between winning a private sector contract or losing one.

- **Compliance with Other Applicable Regulations and Frameworks**

  Many companies in the United States including DoD Contractors fall under multiple cybersecurity requirements. Meeting CMMC Level 3 requirements can also help you meet some or all of the requirements under other regulations and frameworks including:

  - PCI DSS
  - HIPAA Security Rule
  - The NIST Cybersecurity Framework
  - ISO 27001
  - NYS DFS Cybersecurity Regulation

  Finally, CMMC represents a new frontier in government efforts to ensure that federal contractors have implemented adequate cybersecurity. It is highly likely that in the coming years, additional agencies may add similar requirements to RFP's in order to compete for their contracts. Proactively meeting CMMC Level 3 will likely help your organization meet many, if not all, future requirements that other agencies may propagate.

When do I need to receive CMMC certification?

DoD is working expeditiously to begin the rollout of CMMC by the end of 2020, however, the pandemic may cause some unexpected delays on this front. Full implementation of CMMC will likely begin over a gradual rollout ending in 2025. DoD expects over half of primary and subcontractors will be assessed by 2022.

If you are a defense contractor with questions about preparing for CMMC certification, call CAETRA and schedule a CyMetric demo today.