BitLyft
Cybersecurity

CMMC

COMPREHENSIVE GUIDE

Understanding the cybersecurity requirements for doing business with the DoD.

TABLE OF CONTENTS

Executive Summary 3
Introduction to CMMC 4
What is the CMMC? 5
Clarifying CMMC 6
17 Compatibility Domains 6
5 CMMC Levels 7
3PAO Certification 9
Comparing NIST to CMMC 10
Who does CMMC apply to? 12
CMMC for Manufacturing 12
CMMC for Higher Education 13
How Do I Become CMMC Certified? 14
The Bottom Line 17

EXECUTIVE SUMMARY

For many contractors, subcontractors, higher education institutions, and a variety of other organizations, Cybersecurity Maturity Model Certification (CMMC) is surrounded by a considerable amount of stress and confusion. Learning exactly how CMMC directly affects you, and how to obtain the level of certification you need, can easily get lost in the details. While the process might not be a walk in the park, reaching your desired level of CMMC is possible, and it can help your organization avoid dangerous security gaps. You need a comprehensive CMMC guide.

Learning all the details of CMMC, why it's a necessary cybersecurity measure, and how to get started with the certification process can help you prepare to meet your CMMC goals. This article is designed to provide a CMMC guide. You can quickly access all the details you need to educate your organization and get started on the path to certification.

BitLyft
Cybersecurity

INTRODUCTION TO CMMC

To get a firm understanding of the CMMC and the associated responsibilities of your organization, the best place to start is an introduction. The CMMC, or Cybersecurity Maturity Model Certification, is a certification procedure developed by the Department of Defense to certify that contractors working with the department have the necessary controls to protect sensitive data. This data is referred to as controlled unclassified information (CUI), and many organizations that work with the DoD or are subcontractors for companies that work with the DoD must use, store, and share this information while carrying out the terms of a contract.

The CMMC is a framework designed to provide organizations with the necessary regulations to perform basic cybersecurity tasks. This keeps sensitive information out of the hands of threat actors. CMMC is composed of 17 domains that make up five levels of security ranging from basic hygiene to state-of-the-art cybersecurity. Most organizations will not be required to meet all five levels of certification.

The CMMC is based on NIST standards that many affected organizations are already somewhat familiar with. However, there is no self-certification option for CMMC. Instead, organizations must gain certification through a third-party assessment organization (3PAO).

OVER 300,000 ORGANIZATIONS ARE LISTED IN THE DEFENSE INDUSTRIAL BASE (DIB), AND WILL NEED TO BE CERTIFIED UNDER CMMC BY 2025.

WHAT IS THE CMMC?

If you're still feeling confused, don't be alarmed. We're just getting started. As a DoD contractor, you've likely had some experience with NIST guidelines and some of the general confusion surrounding implementation of proper cybersecurity measures. CMMC combines NIST and other standards into a unified standard for cybersecurity. Technically, many of these standards aren't new. They're simply divided into five levels to allow organizations to put measures in place to reach the minimum cybersecurity necessary to protect CUI used within each department. The addition of 3PAO certification provides proof that any organization working with the DoD has the proper security measures in place before winning a contract.

Essentially, CMMC is a program that provides contractors and organizations collaboration with the DoD as a long-term solution to learning. Furthermore, this CMMC guide informs effective cybersecurity measures that will adequately protect government information. When the phased roll-out is complete (September 30, 2025) every organization that works with the DoD or subcontracts under a contract for the DoD will have to reach some level of CMMC. It's also important to note some contracts will include CMMC requirements immediately, with the number of CMMC compatible contracts growing along the way.

In the past, organizations have had time to create a cybersecurity improvement plan while working on DoD contracts. CMMC works differently. Contractors will need to be certified before bidding on contracts. This means each organization will need time to prepare long before the final rollout phase. Since some companies are already observing NIST standards, preparedness for CMMC will vary widely. An assessment to determine the gap between your current cybersecurity practices and your target CMMC level can help you prepare for certification.

The phased rollout of CMMC is designed to give all organizations the time they need to properly apply practices needed to plan, implement, and carry out a robust cybersecurity plan. Instead of using this time to put off certification, it's important to plan and find ways to achieve certification as soon as possible. As more DoD contracts require CMMC compliance, organizations still struggling to prepare for an audit will fall behind. Failure to achieve compliance will result in the inability to bid on and win DoD contracts. Plan to use at least six months to prepare your organization for the CMMC audit. This will provide you with certification for your target level of compliance.

Essentially, CMMC is a program that provides contractors and organizations collaboration with the DoD as a long-term solution to learning. Furthermore, this CMMC guide informs effective cybersecurity measures that will adequately protect government information. When the phased roll-out is complete (September 30, 2025) every organization that works with the DoD or subcontracts under a contract for the DoD will have to reach some level of CMMC. It's also important to note some contracts will include CMMC requirements immediately, with the number of CMMC compatible contracts growing along the way.

CLARIFYING THE CMMC

A major part of preparing for CMMC compliance is determining your target level of compliance. The purpose of creating a framework with five levels is to allow organizations to match their security level with potential risks. Instead of each organization facing the burden of Level 5 CMMC, most organizations will only need to comply with the standard outlined in the first three levels. Determine your target CMMC level and the actions you'll need to take for certification. It helps to understand the structure of the CMMC.

CMMC is made up of 17 capability domains that make up five levels of security. Each level builds off levels before it, so every organization will have to begin by reaching Level 1 CMMC. Any organization compliant with Level 5 CMMC will also have every standard in place to be compliant with lower levels as well.

17 COMPATABILITY DOMAINS

There are 171 practices and 5 processes across the five levels of CMMC maturity, These practices and processes are broken up into 17 capability domains to make them more manageable.

- Access Control
- Asset Management
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Recovery
- Risk Management
- Security Assessment
- Situational Awareness
- Systems and Communications Protection
- System and Information Integrity

5 CMMC LEVELS

01

Level 1: Basic Cyber Hygiene:

Includes 17 practices derived from NIST standards. Level 1 requires a performance-only approach to cybersecurity. These standards are basic cybersecurity practices most companies should already be using when working for the DoD.

02

Level 2: Intermediate Cyber Hygiene:

Includes 72 practices with 55 new standards and 17 from level 1. Level 2 is a big step up from level 1 in that an organization is expected to establish and document standard operating procedures, policies, and strategic plans for its cybersecurity plan.

03

Level 3: Good Cyber Hygiene:

Includes 130 practices. This level will be required of any organization that handles, uses, or shares CUI. Level 3 certification requires the addition of incident reporting and the ability to demonstrate the management of practice implementation.

04

Level 4: Proactive:

Includes 156 practices and generally indicates a more advanced cybersecurity system. Many organizations won't be required to reach level 4 CMMC. A level 4 organization is expected to review and document activities for effectiveness and inform high-level management of any issues.

05

Level 5: Advanced/Progressive:

Includes 171 practices and is the highest level of CMMC compliance. Level 5 organizations have an advanced, progressive cybersecurity system in place. These organizations will have the ability to assess advanced threats and optimize tools to repel these threats.

5 CMMC LEVELS CONTINUED

These numbers seem intimidating, but it's important to remember that they compound off one another. For instance, instead of 72 additional practices for level 2, you'll be adding 55 to the 17 already implemented in level 1. Additionally, the practices aren't new, they're reiterations of practices from Federal Acquisition Regulation (FAR) 48 CFR 52.204-21 and NIST SP 800-171r1 and Draft NIST SP 800-171B. The processes are more loosely defined, and change with each of the five levels as follows.

- Level 1- performed
- Level 2- documented
- Level 3- managed
- Level 4- reviewed
- Level 5- optimized

BY 2025, ALL DoD SOLICITATIONS AND CONTRACTS WILL REQUIRE CMMC COMPLIANCE.

3PAO CERTIFICATION

The elimination of self-certification is one of the biggest changes from NIST qualifications. It's a concern to many organizations worried about preparing for certification and grappling with the costs of getting in shape. In the past, self-certification with DFARS has led to a struggle for many contractors. Since many NIST requirements are extensive, they've been known to lead to more than one interpretation. For some, improper interpretation could result in false claims and non-compliance fines and penalties.

CMMC requires all organizations to be certified by an approved third-party organization. This action could help minimize confusion surrounding the actions necessary to achieve and maintain cybersecurity compliance. However, it does nothing to ease the burden of potential performance risks associated with cybersecurity. Even with the right security measures in place, no organization can guarantee its network will never be breached.

The actions taken by the DoD in the event of a cybersecurity incident are unknown, but loss of certification is anticipated. This means that organizations aren't only shouldering the costs of achieving compliance, but can also be expected to continually improve security measures in the future.

As organizations prepare for the phased rollout, it can be comforting to understand DoD intends to implement the program in a crawl, walk, run sequence by gradually introducing CMMC requirements to new contracts. No current contracts will be modified to include the CMMC regulations.

COMPARING NIST TO CMMC

For contractors familiar with the use of NIST standards, CMMC will be more than a little familiar. After all, NIST provides a major part of the framework used to create CMMC. However, CMMC is designed to take cybersecurity a step further and help eliminate some of the confusion and lack of success surrounding the implementation of NIST.

While CMMC and NIST are both parts of the complete cybersecurity package and use many of the same standards, NIST compliance doesn't necessarily equal CMMC compliance. Perhaps more surprisingly, the reverse isn't necessarily true either. CMMC compliance doesn't ensure NIST compliance. For many organizations, this is where the confusion comes in. Luckily, it doesn't mean that contractors will have double the amount of cybersecurity standards that existed in the past. In many ways, NIST and CMMC overlap and complement each other. To get a better understanding, it helps to compare the similarities and differences between NIST and CMMC.

SIMILARITIES OF NIST TO CMMC

- Level 1 CMMC is completely composed of NIST standards.
- The implementation of NIST and CMMC are both derived from DFARS.
- Complete compliance with NIST SP 800-171 provides many of the requirements for Level 3 CMMC.
- Your MSSP can help you prepare for and manage the cybersecurity requirements for both NIST and CMMC.

DIFFERENCES: NIST & CMMC

- CMMC includes levels of compliance that provide some organizations with fewer requirements.
- CMMC requires third-party certification with no options for self-certification.
- Compliance with CMMC is required to even bid on contracts.
- Subcontractors must be able to prove compliance instead of depending on primes for certification.
- Non-compliance will come with a higher cost.
- CMMC has practices and domains added that go beyond NIST standards.
- CMMC adds practice maturity which requires organizations to create a policy instead of simply applying controls and processes.

While all the additional requirements imposed by CMMC feel cumbersome at first, many of them are designed to take the guesswork and failures out of cybersecurity compliance. The goal is to make implementation simple enough to create a complete security system for every organization working with the DoD.

For instance, separating CMMC into five levels eliminates the need for organizations to achieve security standards that extend far beyond their risks. The breakdown also makes the entire process easier to navigate for those striving for higher levels of compliance. The CMMC essentially adds structure to NIST guidelines that provide clear instructions for a solid cybersecurity solution.

WHO DOES CMMC APPLY TO?

Eventually, CMMC will apply to every contractor, subcontractor, company, organization, higher learning institution, and any other facility that works with the DoD. This is a broad category, but it has been deemed necessary to keep CUI and other sensitive government information protected against cybercriminals. While the contractors and subcontractors associated with the DoD potentially fall under a variety of industries, higher education institutions, and manufacturing companies will be among the most heavily impacted by CMMC.

MANUFACTURING

For manufacturing companies that already work with the DoD, CMMC compliance is probably the number one thing on your to-do list. Manufacturers that routinely win contracts with the DoD depend heavily on the income and business growth they provide. Simply put, all manufacturers and suppliers who sell to the DoD will have to achieve some level of compliance. While CMMC will replace the need for self-certification, it doesn't replace DFARS regulations. Instead, CMMC requirements act as a supplement to DFARS regulations.

Manufacturers who depend on DoD contracts should take careful inventory of when contracts must be renewed and which contracts include the handling of CUI. While existing contracts won't be affected by CMMC, new ones could be affected as early as 2021. After determining your target level of compliance, you'll need to conduct a gap analysis to determine how much work needs to be done to prepare for your audit.

CMMC FOR HIGHER EDUCATION

Higher education institutions are no strangers to governmental compliance requirements. Unfortunately, this doesn't make CMMC easier to obtain. Many of the typical regulations for higher ed organizations surround the privacy of personal information. CMMC has different requirements which often surround research, and may not affect the entire facility. Many higher education institutions hoped to avoid CMMC entirely, but it's not likely there will be any exemptions. For many higher education institutions, the implementation of CMMC standards for at least part of the organization is likely.

> With the right assistance, higher education institutions can not only avoid the penalties of non-compliance, but some organizations can also gain advantages by achieving compliance early.

If your institution handles DoD-sponsored research, you'll need to identify the type of information the facility is responsible for, the localized environment, and the current security practices used to protect this information. Identifying the localized environment provides a clear picture of the environment that will be required to adhere to CMMC guidelines. Most higher education institutions will be seeking Level 1 or Level 3 CMMC. To determine which applies to your research center, you'll need to determine if any DoD contracts require the handling of CUI. To perform a gap assessment, many organizations will require the assistance of a third-party MSSP provider.

HOW TO BECOME CERTIFIED

To become CMMC certified, you must be audited by a certified third-party assessment organization (C3PAO) or an accredited individual assessor. However, for most companies, it would be a mistake to assume you should begin with the audit. Preparing for an audit will likely require considerable planning and the implementation of cybersecurity practices outlined by the CMMC standards. Investigating your current cybersecurity practices and determining the changes you need to make will help you prepare to pass the audit. CMMC compliance at any level can be a challenge. Take these steps to achieve your target level through a comprehensive CMMC guide.

Start Early

The DoD designed CMMC to be completed on a phased rollout for a reason. Waiting for the final deadline to seek certification would likely put you behind other companies interested in the same bids. Proper implementation of cybersecurity practices will require a timeline to evaluate and reform your security weaknesses before scheduling an audit. Additionally, a delay in the audit schedule should be anticipated. With a slow start due to COVID-19, and approximately 300,000 contractors and subcontractors requiring compliance, auditors are likely to be busy.

Perform a Gap Assessment

A readiness assessment (gap assessment) is the best way to determine the difference in your current cybersecurity plan and where you need to be to achieve compliance at your desired level. A readiness assessment performed by a third-party cybersecurity company will examine current cybersecurity practices and uncover inadequate systems and processes that fail to meet minimum CMMC requirements for a given level. The gap assessment will provide you with the information you need to create a remediation plan.

Create a Remediation Plan

Applying a successful remediation plan is key to passing your audit and achieving your desired level of compliance. This is your chance to get everything in place and working properly before it's time for your audit. With a complete gap analysis, you or your MSSP provider can identify risks, prioritize activities, and determine costs for any remedial steps required for CMMC certification.

Your remediation plan will address gaps and outline the plans and resources needed to resolve them. The plan should also provide an actionable timeline to complete your goals. Your current implementation of cybersecurity-best practices and your target level of CMMC will guide exactly how involved your remediation plan needs to be.

Practice Ongoing Cybersecurity

Successful cybersecurity requires more than just a plan. Ongoing cybersecurity practices require a changing process with the ability to monitor, detect, and report on cybersecurity incidents in an evolving technological atmosphere. As you adjust to your changing and growing cybersecurity practices, you can address vulnerabilities and update your security plan to include this knowledge. Your CMMC assessment will require the most updated version of your cybersecurity plan and processes.

Scheduling Your CMMC Audit

Your CMMC audit must be performed by a certified 3PAO. To find a certified assessor, you'll need to visit the CMMC-AB Marketplace website. and choose a 3PAO from the list of Authorized and Accredited C3PAOs. You'll schedule your audit. When the audit is performed, you'll either pass the assessment or address security gaps found by the assessor. When your CMMC level is achieved, your certification will be valid for three years.

Achieving CMMC compliance is a challenging process for many organizations, especially small to medium businesses that are less familiar with NIST guidelines. However, these guidelines are necessary to maintain the required cybersecurity level to protect sensitive government information.

Preparation is key for a successful CMMC audit. For companies without a complete in-house cybersecurity team, it's generally more cost-effective to contact a third-party cybersecurity expert to help you prepare for your CMMC audit. To learn more about CMMC compliance and how to simplify your CMMC journey, get in touch with one of our cybersecurity experts.

Companies must continually reevaluate the specific requirements in WISPs and the program itself at least once every year.

Risk Assessment

Typically, WISPs require organizations to implement policies and practices that can proportionately counter the volume and sensitivity of the available data and the resources they can gather to keep the data safe.

Minimum Tech Security

WISPs require that you have adequate anti-malware software, encryption, and other internal or perimeter defenses within your computer systems.

Staff Training

Implementation alone isn't enough. Staff must be educated on the security requirements and understand the organization's WISP to deliver the expected results. From these requirements, it's clear that WISP is a collection of living practices and not a document aimed at papering an organization's liability.

RECAP

- Start Early
- Perform a Gap Assessment
- Create a Remediation Plan
- Practice Ongoing Cybersecurity
- Scheduling Your CMMC Audit
- Risk Assessment
- Minimum Tech Security
- Staff Training

THE BOTTOM LINE

Your CMMC Guide

By now, you're aware that data is your organization's most precious commodity. Protecting its credibility and security is the primary step of keeping the entire origination safe. WISPs offer the essential procedures, protections, and policies to achieve this objective.

Do you need a comprehensive written information security program tailored to your organization's structure and needs? The Technology Advisory Group is here to help you avoid being an easy target for malicious individuals. Talk to us today to get the proper assistance.

HELPFUL LINKS

- BitLyft Cybersecurity
- Talk to a Cybersecurity Expert
- Continued CMMC Reading

BitLyft
Cybersecurity