C3

CMMC BASICS

An Introduction to Cybersecurity Maturity Model Certification (CMMC)

This comprehensive eBook breaks down the CMMC framework, CMMC levels, and the benefits of certification for organizations in the Defense Industrial Base (DIB)

APPROVED FOR PUBLIC RELEASE — 25042

Table of Contents

An Introduction to Cybersecurity Maturity Model Certification (CMMC)

Introduction

The Cybersecurity Maturity Model Certification (CMMC) program is a framework designed to enforce the protection of sensitive unclassified information that the U.S. Department of Defense (DoD) shares with its contractors and subcontractors.

The CMMC program is aligned to the DoD's information security requirements for the Defense Industrial Base (DIB) to ensure defense prime contractors, subcontractors, and suppliers have implemented the security measures required to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The CMMC program aims to protect the DIB from the growing frequency and complexity of cyber threats.

CMMC requirements apply to any organization that is part of the DoD supply chain or handles sensitive unclassified information related to defense contracts, regardless of their size or specific industry sector. After years of discussion and refinement, the Federal Register published the DoD's CMMC program as a Final Rule in Title 32 of the Code of Federal Regulations (CFR) in October 2024. Title 32 focuses on the technical aspects of the CMMC program, including the certification process and requirements of the program. The complement to Title 32 is Title 48. The proposed final rule for Title 48 was released in August 2024, focusing on government procurement and ensuring the integration of CMMC into contracts. It will include the integration of CMMC into contracts and is expected to be finalized in the first half of 2025. Phase 1 of CMMC will begin on the effective date of Title 48.

Both rules are essential for the successful implementation of CMMC and the protection of sensitive information. As malicious actors and nation states increasingly target the DIB, it is vitally important to protect this information appropriately. (For the latest on the status of rulemaking, refer to these blogs for Title 32 and Title 48.)

In this guide, we'll break down the basics of CMMC and what defense contractors, subcontractors, and suppliers need to know about the program and the requirements of the framework.

Chapter 1: Understanding the CMMC Framework

What Is the CMMC Framework?

The CMMC Framework is a comprehensive cybersecurity standard developed by the DoD to protect sensitive information within the DIB supply chain. It enables the DoD to assess the cybersecurity posture of its prime contractors and subcontractors and verify that they are protecting sensitive information appropriately.

The framework is organized into multiple maturity levels, each more stringent than the previous one. Depending on the level and type of information being handled, meeting CMMC requirements involves either a self-assessment or a third-party certification and will soon become a prerequisite for defense contract eligibility.

Under the CMMC framework, prime contractors must ensure that their subcontractors and suppliers meet the appropriate CMMC level for the type of information they handle, which creates a cascading effect of compliance throughout the supply chain tiers.

At a high level, CMMC defines how sensitive information should be handled and protected at every stage of the supply chain, including marking and controlling the flow of data between tiers. Practically speaking, the framework outlines the requirements of a secure and compliant environment, from the technical controls required to safeguard data to the policies and processes that should be followed to mitigate risk.

While much of the emphasis around CMMC is focused on the achievement of compliance, the framework itself includes provisions to ensure the continued maintenance of a compliant environment and emphasizes ongoing assessment and monitoring as a required component of maintaining defense contract eligibility and managing supply chain risks.

Key Components of the Framework

The CMMC framework includes a comprehensive and scalable certification element designed to verify the implementation of cybersecurity processes and practices. While adherence to cybersecurity controls has been required in defense contracts since December 31, 2017, there has previously been no enforcement element to these cybersecurity controls, resulting in uneven compliance and unwanted exposure of sensitive information.

The introduction of assessment and certification elements—particularly third-party assessments as outlined in Levels 2 and 3 of CMMC—introduces a higher degree of accountability to ensure defense contractors protect sensitive unclassified information adequately and maintain cybersecurity best practices, even across subcontractors in a multi-tier supply chain. Through the assessment process, organizations verify that they have implemented specific processes and practices that safeguard their environments (and the data therein) from attack. While many of these controls reflect basic cybersecurity measures such as multi-factor authentication (MFA) and firewalls, a number of them require a more diligent approach to cybersecurity. The framework can be applied to organizations of all sizes and complexities within the DIB to ensure that both large and small contractors can comply with relevant CMMC requirements. The multiple maturity levels define the different requirements based on the sensitivity of the information the organization seeking assessment processes, stores, or transmits.

Chapter 2: CMMC Levels Explained

While CMMC was initially released for public comment in January 2020, the framework has been significantly adjusted and simplified since its introduction. Today, the final CMMC rule has three levels of cybersecurity, starting at the most basic, Level 1, and culminating in the most advanced, Level 3. Each of these levels corresponds to specific cybersecurity practices and processes that must be implemented to protect **Federal Contract Information (FCI),** which is information that is not intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government, and **Controlled Unclassified Information (CUI),** which is information that requires safeguarding or dissemination controls pursuant to and consistent with federal law, regulations, and government-wide policies.

> **The U.S. National Archives and Records Administration (NARA)** oversees the federal CUI program, clarifying that: "While FCI is any information that is 'not intended for public release,' CUI is information that requires safeguarding and may also be subject to dissemination controls."

One critical note: CMMC Statuses are awarded to an assessed *environment*, not holistically to the organization itself. If an organization seeks multiple contracts, either the assessment scope must be inclusive of activities required for each contract or separate assessments must be conducted.

Level 3

PROTECTION OF CUI AGAINST ADVANCED PERSISTENT THREATS (APTS)

Focuses on reducing risks posed by APTs, with advanced cybersecurity measures to protect CUI. This level applies to contractors playing key roles in defense and incorporates an additional 24 controls from NIST SP 800-172.

Level 2

BROAD PROTECTION OF CUI

Broadly safeguards Controlled Unclassified Information (CUI) by aligning with NIST SP 800-171 Rev 2 standards, incorporating 110 controls.

Level 1

BASIC SAFEGUARDING OF FCI

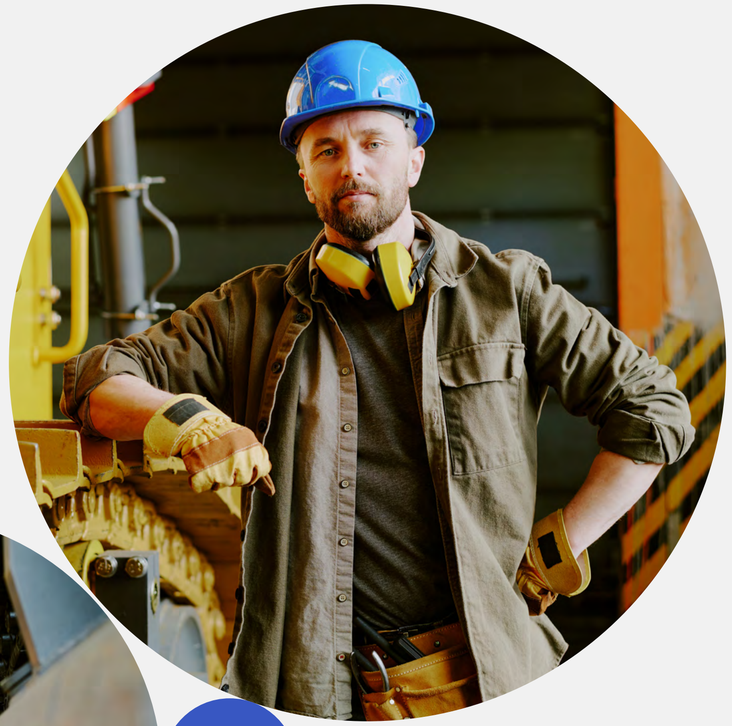
Provides foundational cybersecurity practices to protect Federal Contract Information (FCI) with 15 essential practices as defined in FAR clause 52.204-21.

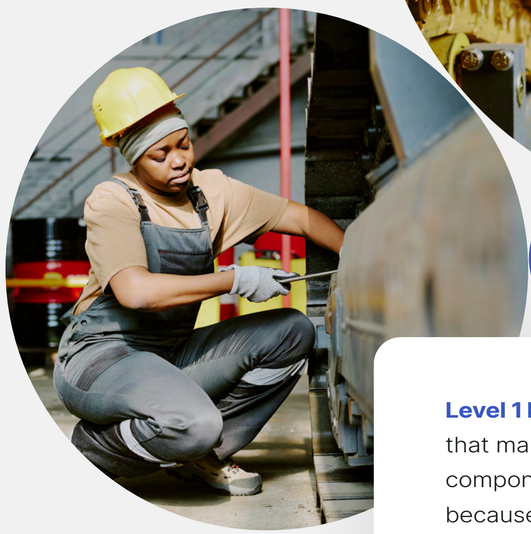
The 3 CMMC Levels

Level 1 — Basic Safeguarding of FCI

Focused on organizations who only handle FCI and do not come into contact with any CUI, Level 1 requires an organization to demonstrate compliance with 15* basic cyber hygiene practices to protect FCI that aligns to 48 CFR 52.204-21, which is commonly known as the FAR Clause. Contractors (and their subcontractors) awarded a Level 1 (Self) contract must self-assess their compliance annually. No exceptions are allowed. Third-party assessments are not required.

Level 1 summary: To ensure that organizations have basic cyber security practices in place, organizations must follow the 15 practices derived from the FAR Clause, including limiting system access to authorized users, controlling physical access to information systems, system and communications protection, and protecting information during disposal.





Level 1 Example Organization: A small machine shop subcontractor that manufactures a commercial, off-the-shelf (COTS) metal component of military equipment needs to comply with Level 1 because they handle specifications and purchase orders (FCI) from the prime contractor, but does not have access to the full design.

*You may occasionally see information that references 17 security requirements for CMMC Level 1. CMMC Level 1's 15 requirements are outlined in FAR clause 52.204-21. When mapped to NIST 800-171 R2, one of those requirements is split into 3 parts, resulting in the 17 number.

Level 2 Example Organization: A defense contractor involved in producing military communication systems needs to comply with Level 2 because design information related to components of the equipment is critical to national security and therefore marked as CUI.

Level 2 — Broad Protection of CUI

Organizations that handle CUI will be required to meet CMMC Level 2. An organization must demonstrate compliance with 110 controls to validate that they have implemented cyber hygiene practices required to protect CUI. The 110 controls are outlined in the National Institute of Standards and Technology (NIST) security requirements and processes in NIST 800-171 r2. (While NIST 800-171 r3 was finalized in May 2024, at this time, the DoD explicitly indicates that the focus for the final CMMC rule is on r2.) These 110 controls cascade into 320 explicit assessment objectives, as outlined in NIST 800-171a r2, against which an organization is measured.

There are two types of assessments available in Level 2, and which assessment is required will be determined by the individual contract being awarded.

01. **Self-Assessment:** Performed by the entity itself, self-assessments are required every three years, with an affirmation of conformance submitted annually by an executive of the contractor. In its January 15, 2025 memo, the Department of Defense indicated that Level 2 self-assessments will only be allowed for “CUI outside of the National Archive’s CUI Registry Defense Organizational Index Grouping.” It’s estimated that only 5% of Level 2 awards will be eligible for self-assessments.

    Regardless, contracts that require a CMMC Status of Level 2 (Self) still require the organization seeking assessment to adhere to NIST SP 800-171 standards r2. Self-assessment results must

be submitted to the Supplier Performance Risk System (SPRS), including CMMC Level, Assessment Date, Score, Commercial and Government Entity (CAGE) codes, and Plan of Action & Milestones (POA&M) status if applicable.

02. **Certification Assessment:** Performed by a Certified 3rd Party Assessment Organization (C3PAO), these formal assessments are required every three years with an affirmation of conformance submitted annually by an executive of the contractor. According to the January 15, 2025 memo, Level 2 certification will be the minimum requirement for any contract that requires the contractor "to process, store, or transmit CUI categorized under the National Archive's CUI Registry Defense Organizational Index Grouping."

Scoring and Status: Both self-assessments and certification assessments use the same scoring system, but result in different designations:

ASSESSMENT TYPE	SCORE: 88-109 "CONDITIONAL STATUS"	SCORE: 110 "FINAL STATUS"
01 ***Self***-Assessment	CMMC Status of Conditional Level 2 (Self)	CMMC Status of Final Level 2 (Self)
02 ***Certification*** Assessment	CMMC Status of Conditional Level 2 (C3PAO)	CMMC Status of Final Level 2 (C3PAO)

Both self-assessments and certification assessments require entities to implement NIST SP 800-171 r2 controls. If the organization achieves a score of 110, they are issued a "CMMC Status" of either "Final Level 2 (Self)" or "Final Level 2 (C3PAO)" depending on the type of assessment conducted.

If their score falls between 88-109 (with caveats, see the note below), they may receive a "Conditional CMMC Status," which will require a POA&M to address any requirements that are scored as NOT MET. Conditional assessment statuses can last no longer than 180 days and all POA&M issues must be resolved in order to achieve the desired final assessment status.

Note: The ability to qualify for a conditional assessment status at Level 2 is in fact quite limited. Of the 320 assessment objectives listed in NIST 800-171a, 215 assessment objectives constitute an "instant failure" if not met at the time of the assessment, with no ability to put them on a temporary POA&M.

Level 2 summary: Organizations must follow 110 controls aligned with NIST SP 800-171, covering fourteen domains. These include Access Control, Awareness Training, Audit and Accountability, Configuration Management, and many more. These practices include user access provisioning, securing application services, event logging, and incident response. The objective is to effectively manage and reduce cybersecurity risks through documented and consistent practices.

Level 3 — Protection of CUI against Advanced Persistent Threats (APTs)

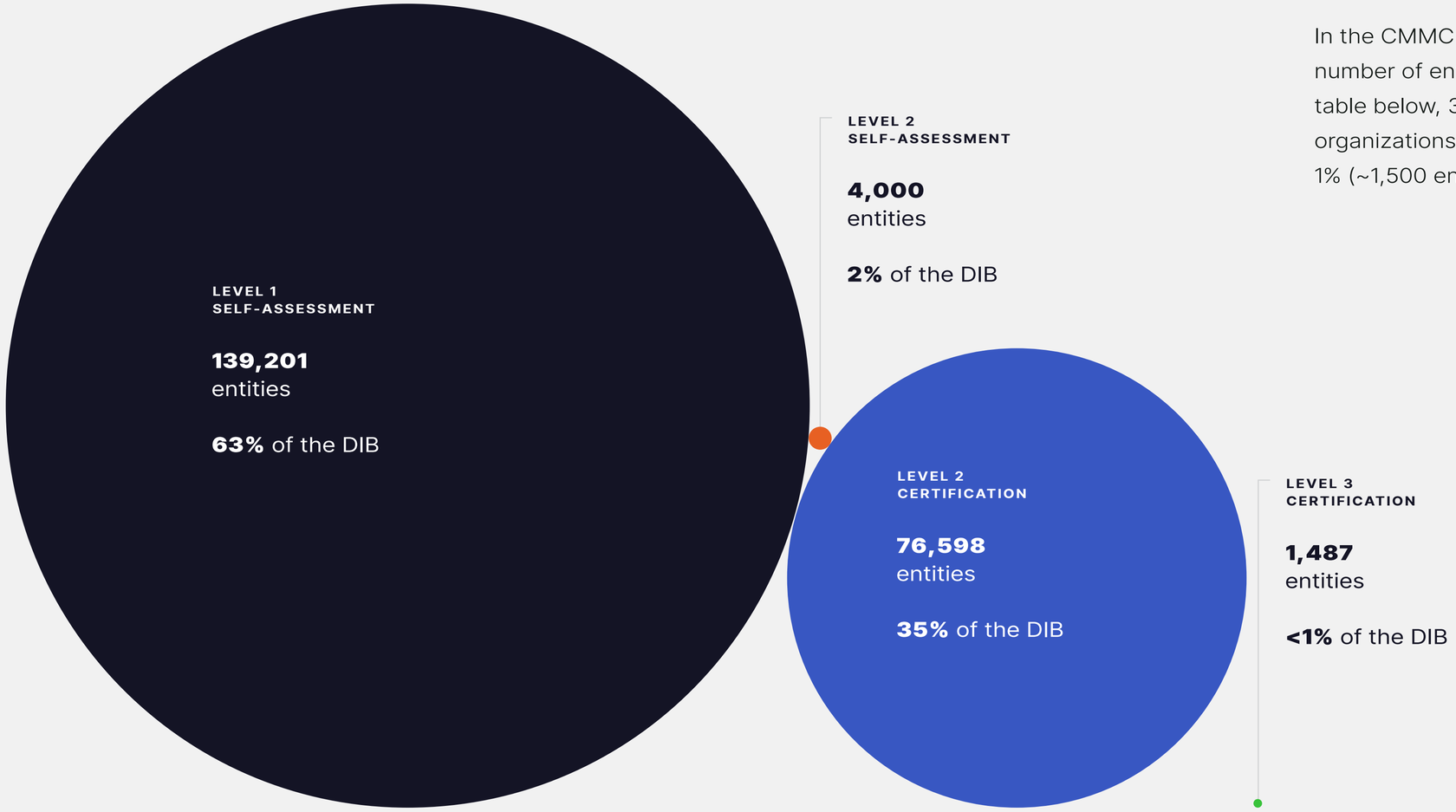
Building on the requirements of Level 2, an organization seeking CMMC Status of Final Level 3 (DIBCAC) must first have achieved a CMMC Status of Final Level 2 (C3PAO) for the relevant environment and then also have standardized and enhanced practices that enable advanced protection against Advanced Persistent Threats (APT)s, such as nation-state actors, and comprehensive safeguarding of CUI. To receive a CMMC Status of Final Level 3 (DIBCAC) the entity must also implement 24 selected security requirements from NIST SP 800-172.

This level is targeted at entities working on the most critical defense programs. Contracts that require a CMMC status of Final Level 3 (DIBCAC) require their scoped environment to undergo an assessment conducted by a team from the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Results will be entered into CMMC Enterprise Mission Assurance Support Service (eMASS), which electronically transmits the results to SPRS. Assessment scores are affirmed by a senior official of the contractor after each assessment, including POA&M closeout, and annually thereafter. Seven of the 24 additional assessment objectives required for Level 3 certification constitute an automatic failure.

> If any Plan of Action & Milestones is not closed out within 180 days, the Conditional Assessment will expire.

Level 3 Example Organization: A defense contractor involved in developing and maintaining critical defense systems, such as missile defense technology, would be an example of a company that may need to comply with Level 3. These systems are high priority due to their strategic importance and the sensitive nature of the information they handle.

Estimated Number of Entities Expected for Each CMMC Level



Level 3 summary: By requiring organizations to implement advanced cybersecurity measures and maintain a robust cybersecurity plan, organizations demonstrate a high level of cybersecurity maturity and resilience against sophisticated threats.

In the CMMC proposed rule, the government provided estimates of the number of entities expected for each CMMC Level. As outlined in the table below, 37% of the Defense Industrial Base—or more than 80,000 organizations—will be subject to Level 2 requirements, with an additional 1% (~1,500 entities) requiring Level 3 certification.

CMMC Level	# of Entities	% of the DIB
Level 1 Self-Assessment	139,201	63%
Level 2 Self-Assessment	4,000	2%
Level 2 Certification	76,598	35%
Level 3 Certification	1,487	1%

Chapter 3: CMMC & NIST 800-171

CMMC aligns closely with NIST cybersecurity standards in several ways, using existing federal regulations, specifically NIST SP 900-171 rev 2 and NIST SP 800-172, to build a unified set of cybersecurity best practices. This ensures that CMMC and NIST share similar language and concepts, which can facilitate clear communication and simplify compliance efforts. In addition to shared terminology and concepts, the focus of the CMMC program on protecting CUI aligns with NIST's risk-based approach to cybersecurity. Both emphasize that cybersecurity practices must be continually improved to keep up with changing technologies and threat vectors. By using the NIST Cybersecurity Framework (CSF) as a foundation, organizations can build a scalable cyber risk management program that aligns with CMMC requirements.

This is particularly true of the more robust requirements of CMMC Levels 2 and 3. CMMC Level 2 directly requires organizations to implement all 110 security controls from NIST SP 800-171, while CMMC Level 3 incorporates additional controls from NIST SP 800-172 for more advanced protection. In addition, the assessment methodology for CMMC Level 2 is mapped to NIST SP 800-171A, which outlines assessment criteria organizations can use to generate evidence that supports the assertion that the security requirements have been satisfied. Using these assessment criteria, organizations can:

- Identify potential problems with internal security and risk management programs
- Identify security weaknesses and deficiencies in systems and those environments in which the systems operate
- Prioritize risk mitigation activities and decisions
- Verify that any identified security weaknesses and deficiencies in environments have been addressed

- Support continuous monitoring activities and enable organizations to have information security situational awareness

CMMC builds on NIST SP 800-171 by adding a structured assessment and certification process using the methodologies in NIST SP 800-171A, enabling a validation mechanism to ensure companies are meeting their contractual obligations.

Understanding Domains in CMMC

NIST 800-171 outlines 14 security families (or domains). The domains provide a structured approach to implementing and assessing cybersecurity practices for organizations seeking CMMC certification. Each domain refers to a broad area of cybersecurity protection; while the number of practices within each domain vary, the domains cover multiple aspects of cybersecurity to ensure comprehensive protection of CUI in the DIB.

The following 14 CMMC domains are groups or categories of cybersecurity practices that are based on the control families outlined in NIST SP 800-171. The control families group related controls together into domains, making it easier for organizations to allocate resources and expertise on specific areas.

01. **Access Control (AC): 22 controls in Level 2**
The Access Control domain includes the largest number of controls, all designed to limit and manage access to systems, information, and resources.

02. **Awareness & Training (AT): 3 controls in Level 2**
The Awareness & Training domain is focused on the importance of ongoing education and practical exercises to keep personnel informed about current cybersecurity threats and best practices for protecting sensitive information.

03. **Audit & Accountability (AU): 9 controls in Level 2**
This domain includes controls for maintaining and reviewing detailed records of system activities and user actions to ensure accountability.

04. **Configuration Management (CM): 9 controls in Level 2**
Controls in this domain focus on establishing and maintaining control over system configurations, enabling more control over all organizational systems.

05. **Identification & Authentication (IA): 11 controls in Level 2**
This domain ensures organizations can properly identify and authenticate users before granting access to systems, information, and resources.

06. **Incident Response (IR): 3 controls in Level 2**
The Incident Response domain focuses on an organization’s ability to detect, respond to, and recover from cybersecurity incidents and includes testing those capabilities.

07. **Maintenance (MA): 6 controls in Level 2**
The controls in this domain require organizations to maintain organizational systems to protect against security vulnerabilities and ensure system integrity.

08. **Media Protection (MP): 9 controls in Level 2**
The Media Protection domain controls are designed to secure information stored on different types of media and limit access to authorized users.

09. **Personnel Security (PS): 2 controls in Level 2**
These domain controls relate to ensuring that individuals with access to sensitive

information are trustworthy and systems containing CUI are only accessible when necessary.

10. **Physical Protection (PE): 6 controls in Level 2**
    The Physical Protection domain focuses on safeguarding systems, equipment, and the facilities housing them from physical threats and unauthorized access.

11. **Risk Assessment (RA): 3 controls in Level 2**
    Controls in the Risk Assessment domain require organizations to identify, analyze, and manage cybersecurity risks to the organization's systems and information.

12. **Security Assessment (CA): 4 controls in Level 2**
    These controls enable an organization to evaluate the effectiveness of its security controls and identify vulnerabilities in systems and processes.

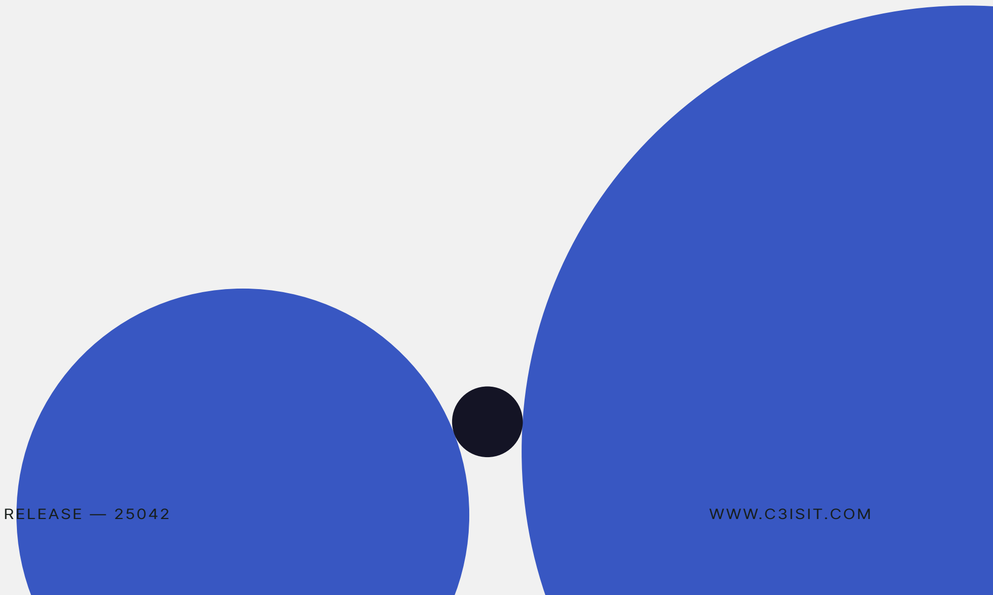
13. **System and Communications Protection (SC): 16 controls in Level 2**
    The controls in this domain focus on protecting the confidentiality, integrity, and availability of information as it is processed within systems and networks.

14. **System and Information Integrity (SI): 7 controls in Level 2**
    The controls in this domain focus on maintaining the integrity of systems and information by monitoring, identifying, updating, reporting, and correcting information and system flaws in a timely manner.

Understanding Controls in CMMC

Within each domain, there exists a number of controls required for each Level. The three CMMC levels naturally have different expectations of the controls required. CMMC Level 1, for example, requires adherence to controls in only seven of the 14 domains, whereas Level 2 has a total of 110 controls across the 14 cybersecurity domains. Most of these controls are separated between basic security requirements, which provide the fundamental security controls, and derived security requirements, which provide more detailed and specific security practices to enhance and support the basic controls.

During CMMC assessments, controls are scored as ***met, not met,*** or ***not applicable.*** A small number of security requirements may be eligible for a POA&M if an assessment shows that they are not fully implemented, and such POA&M items must be closed out within 180 days for a final certification to be issued.



Understanding Assessment Objectives in CMMC

Assessment objectives are part of the CMMC assessment guides, providing detailed information for each practice in the CMMC model.

Even after a CMMC Status has been achieved, the DoD has the right to investigate, and even to conduct a DIBCAC assessment, if there are indications that an active CMMC status has been called into question. The DIBCAC results will take precedence over any previous CMMC status, and if the CMMC status has not been maintained, standard contractual remedies will apply."

Level 1

The proposed CMMC Rule indicates that a CMMC Level 1 Self-Assessment must be performed using the assessment objectives defined in NIST SP 800-171A, modified for FCI instead of CUI, and specific to the 15 controls relevant for CMMC Level 1. There are 59 assessment objectives mapped to the 15 security requirements from FAR 52.204-21 paragraph (b)(1) for CMMC Level 1, providing specific criteria for evaluating compliance with each CMMC practice. They include discussion of the practice, implementation examples, potential assessment considerations, and key references. Organizations use these assessment objectives to determine whether they meet the requirements for CMMC Level 1 during the self-assessment process.

Level 1 self-assessments are effectively pass/fail. Should any control not be achieved, the contractor will remain ineligible for new awards.

Level 2

There are 320 assessment objectives aligned with the 110 security requirements from NIST SP 800-171 for CMMC Level 2. The assessment objectives are clearly outlined in NIST 800-171A, and are used for evaluating compliance to determine whether the organization meets the requirements for certification. Most organizations will need to evaluate compliance with CMMC Level 2 through C3PAOs rather than through self-assessment. Assessment methods include examination, interviewing, and testing as well as reviewing policies, procedures, system security plans; conducting interviews with personnel; and asking key personnel to demonstrate controls.

The achievement of the associated assessment objectives will determine whether a given security requirement is scored as met. The proposed CMMC rule outlines very limited conditions under which a POA&M may be allowed, but again, two-thirds of the assessment objectives (215 out of the 320) have no ability to be remediated through a POA&M.

Level 3

CMMC Level 3 is the highest level in the CMMC framework and is designed for organizations with access to the most critical national security information, requires the achievement of CMMC Status of Final Level 2 (C3PAO) on the Level 3 assessment scope, and then adds 24 selected requirements from NIST SP 800-172 to incorporate additional practices with more stringent assessment objectives. These assessments must be conducted every three years and only by assessors from the DoD. The results must be affirmed by a senior level representative from the contractor who is responsible for ensuring its compliance after each assessment, including closing out the POA&M (if applicable), and annually thereafter.

Chapter 4: Benefits of Early CMMC Certification

Now that the CMMC rule is final, the timeline for implementation is based on the finalization of Title 48, which governs the inclusion of CMMC into the contracting process. Based on the pace of the rulemaking process to date, CMMC Phase 1 will likely take effect by Summer of 2025, with Level 1 and Level 2 self-assessments taking immediate effect for all applicable contracts as a condition of contract award. What that timeline doesn't reflect, however, is the cascading effect of subcontractors' compliance status on their prime contractors. As a result, many primes will require their subcontractors to be compliant ahead of any expected contract award.

While all contractors doing business related to the DoD will have to adhere to CMMC requirements sometime in the next few years, organizations that do so earlier are likely to realize multiple competitive advantages by accelerating their CMMC certification process, including:

- Enhanced market access and competitive differentiation
- Increased trust and credibility and improved supplier relationships
- Improved cybersecurity posture and better risk management
- Broader regulatory compliance
- Long-term cost savings

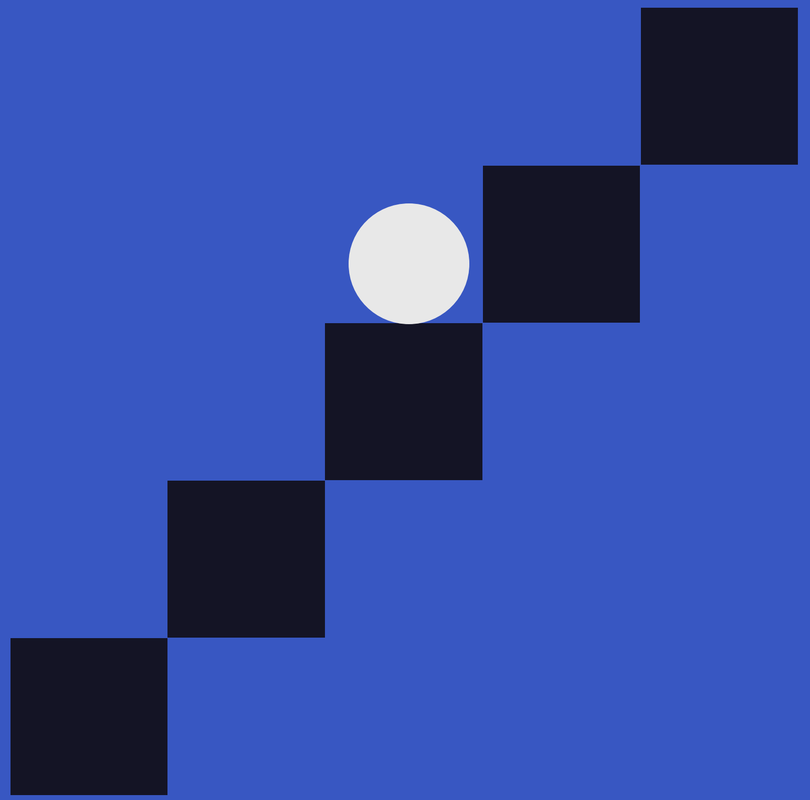
Early adopters of CMMC are likely to realize significant benefits simply because the pool of eligible contractors is smaller. CMMC certification positions these organizations to bid on and participate in government contracts, standing out from competitors that have not yet completed certification. Additionally, larger contractors are sure to actively seek CMMC-compliant subcontractors to work with, not only because it reduces risk and ensures alignment on cybersecurity processes but ensures they won't have to seek new subcontractors when the requirements become official.

In addition to being eligible for more contracts, certification increases trust and credibility by demonstrating a commitment to protecting sensitive information, specifically information designated as FCI and CUI. These benefits extend beyond working with the defense sector, by building trust with other customers, partners, and regulatory bodies – or any other organization concerned about cybersecurity and deterring threat actors. By not only implementing the controls required for CMMC but validating that these practices are functional through assessments, organizations improve both their overall cybersecurity posture and risk management.

Regardless, the DoD has made it clear that it expects the DIB to take cybersecurity seriously. While adherence to NIST 800-171 has been in contracts since 2017, the finalization of the CMMC rule and recent Department of Justice actions related to the False Claims Act have put teeth into the long-standing cybersecurity requirement. And although some organizations may fear that the initial investment in achieving compliance will be substantial, the long-term benefits of improved cybersecurity can lead to significant cost savings, both through eligibility for new DoD contracts and by preventing expensive data breaches and the associated costs of recovery and penalties.

Conclusion

The CMMC program is designed to protect sensitive information in the Defense Industrial Base supply chain. It now enforces a standardized approach to cybersecurity for contractors and subcontractors that closely aligns with the NIST framework for protecting FCI and CUI.



Next Steps

01. Determine the appropriate CMMC level based on the type of information handled (FCI or CUI).
02. Identify your target date for compliance.
03. Identify the resources (or partner) that will help you achieve CMMC. This will include CMMC-savvy systems architects, IT personnel, cybersecurity experts, and compliance consultants.
04. Identify your compliance boundary.
05. Create plans for meeting the technical and non-technical requirements outlined in CMMC.
06. Implement the controls, policies, and procedures required.
07. Validate the controls and collect evidence and documentation required to prove compliance.
08. Complete and submit a self-assessment (for Level 1 or some Level 2 organizations) or schedule an assessment with a C3PAO (for Level 2) or prepare for a government assessment (for Level 3).

This program helps safeguard national security interests by minimizing potential vulnerabilities in the defense supply chain and protecting against increasingly sophisticated cyber threats. By complying with CMMC requirements and getting certified under the newly revised program, defense contractors can gain a competitive edge in the market while contributing to the overall security of the nation's defense infrastructure.

Additional Resources

CMMC Level 2 Controls & Assessment Objectives

Explore the critical cybersecurity controls and assessment objectives necessary for achieving CMMC Level 2 compliance, guided by NIST 800-171 and 800-171A, visualized by C3.

CMMC Final Rule Basics: What You Need to Know

Discover the key updates in the CMMC Final Rule, including streamlined assessments and implementation timelines. This guide is essential for defense contractors preparing for compliance in the evolving cybersecurity landscape.

Title 48 Proposed Rule: CMMC Takes Another Step Forward

The CMMC program took another major step with the publication of the Title 48 proposed rule on August 14, 2024. This rule aims to incorporate CMMC requirements into DoD contracts, complementing the earlier Title 32 rule.

About C3

C3 accelerates CMMC cybersecurity compliance by designing, implementing, and managing IT & cybersecurity solutions purpose-built for the U.S. Defense Industrial Base.

C3 offers a wide range of compliance-centric managed IT services—from targeted services customized to fit within a client's existing environment to the C3 Suite, a set of packaged solutions, including fully managed CMMC offerings purpose-built to meet compliance requirements.

By rooting our prescriptive solutions in cybersecurity best practices and an intimate understanding of CMMC assessment requirements, the C3 Suite minimizes the risk of non-compliance and accelerates compliance timelines, enabling defense contractors to more easily achieve and maintain CMMC Level 2 compliance with confidence.

A leading provider of Microsoft 365 GCC High and Azure Government, C3 is a leading AOS-G Partner, a CMMC Registered Provider Organization (RPO), and one of the few companies to successfully support the DIBCAC assessment of a CMMC Third-Party Assessment Organization (C3PAO).

Visit us at: c3isit.com