DATALOCKER®
SIMPLY SECURE

EBOOK

WHAT IS CMMC 2.0?

TABLE OF CONTENTS

SECTION 1
WHAT IS CMMC 2.0?

Established by the United States Department of Defense (DOD), the Cybersecurity Maturity Model Certification (CMMC) is a framework designed to fortify the cyber defenses of government contractors. The program aims to safeguard confidential information within the DOD supply chain by requiring comprehensive third-party assessments of the security practices of both contractors and subcontractors alike. In essence, CMMC outlines the specific IT security standards businesses must satisfy in order to secure lucrative government contracts.

CMMC was introduced in response to a string of security breaches targeting sensitive federal data. The high profile nature of those exploits led the DOD to reexamine the security capabilities of its ecosystem. The agency determined that the insufficiency of current standards, combined with the lack of accountability from resource-strapped subcontractors rendered the supply chain extremely vulnerable to cyber threats.

CMMC

CMMC WAS INTRODUCED IN RESPONSE TO A STRING OF SECURITY BREACHES TARGETING SENSITIVE FEDERAL DATA.

CMMC IS DEFINED BY ITS THREE CORE PRINCIPALS:

MATURITY LEVELS

DIB entities are required to meet compliance standards at levels that become increasingly stringent depending on the sensitivity of the data in their possession.

THIRD-PARTY AUDIT REQUIREMENTS

CMMC assessments are required to verify and validate the proper implementation of IT security standards defined by the DOD.

MANDATORY COMPLIANCE

In order to secure work with the DOD, companies must achieve full compliance at the CMMC levels specified in the contract.

THE NEED FOR CMMC

Cyber attacks have grown in frequency and gravity as technology continues to advance. In attempt to mitigate the issue, the DOD implemented the NIST SP 800-171 framework, a set of standards that encouraged stronger security practices among government contractors. Despite being rooted in good intentions, the initiative was doomed to fail. Compliance was based on in-house assessments conducted by each individual contractor. With no viable way to measure adherence and cyber security prowess, the standard was only loosely adopted, which proved problematic as the threat landscape evolved.

NIST SP 800-171

THE NIST SP 800-171 FRAMEWORK, A SET OF STANDARDS THAT ENCOURAGED STRONGER SECURITY PRACTICES AMONG GOVERNMENT CONTRACTORS.

The uncertainty of NIST SP 800-171 inspired the DOD to seek out alternatives. In 2019, the agency unveiled the CMMC, a framework modeled after NIST SP 800-171 and other regulatory standards mandated to industries beyond the government realm. While the new standard offered the third-party visibility the previous program lacked, the idea of CMMC was largely met with confusion in regard to the requirements.

A NEW AND IMPROVED STANDARD

In November, 2021, the DOD introduced a revamped cyber security initiative in CMMC 2.0. The updated standard promised to retain the core objectives of the original program, with an added focus on clarifying and simplifying the requirements that seemed to leave the collective Defense Industrial Base (DIB) with more questions than answers. In addition to eliminating specific certification tiers, CMMC 2.0 places greater emphasis on self-policing by reducing the role of third-party auditing.

Although contractors and subcontractors are still accountable for fostering a secure operational environment, the addition of independent assessments will enforce a greater sense of culpability to ensure adequate security measures are met across the supply chain before contracts are awarded.

Upon introducing the first iteration of CMMC, the DOD had aspired to grant a total of 15 pilot contracts as a means to test its assessment process before embarking on the 2025 compliance deadline. With 2.0 added to the equation, the department has opted to forgo the piloting program and more notably, remove CMMC compliance from contractor obligations until the updates are formally integrated into federal legislation.

CMMC 2.0 has been praised for its approach to prioritizing cyber security initiatives in the DIB space, while giving small and medium-sized businesses an easier path to compliance. In the meantime, the DOD is using a combination of rulemaking and input via a public comments period to finalize the revised framework. Needless to say, CMMC is a developing standard every contractor needs to keep locked on their radar.

SECTION 2

WHO NEEDS CMMC CERTIFICATION?

The bidding arena for government contracts is fiercely competitive. However, security compliance can make winning those attractive bids a rather complex and costly proposition. This conundrum is further compounded by evolving requirements that are as dynamic as the attacks they strive to foil.

CMMC demands that all companies obtain certification via an exhaustive assessment process in order to secure future contracts with the DOD. The new standard goes beyond auditing. From people to processes, it's a game-changing revelation that will dramatically affect some of the most important aspects of federal business.

CMMC BUSINESS IMPLICATIONS

CMMC is poised to have major implications for companies across multiple industrial verticals. Let's take a deeper look at the impact the new standard could have on entities in the market for government contracts.

> ***IT IS UP TO CERTIFICATION-SEEKING FIRMS TO DEVISE A TOP-DOWN GAME PLAN THAT PRIORITIZES CMMC AWARENESS, AND ULTIMATELY FOSTERS A CULTURE OF COMPLIANCE ACROSS THE ORGANIZATION.***

Mandatory Audits: Once CMMC 2.0 goes into effect, existing and prospective DOD contractors will not be allowed to secure, or even bid on new acquisitions without achieving certification. Compliance will be validated through independent parties carefully selected and approved by the DOD.

Maturity Requirements: The tiered compliance model is a key facet of CMMC certification. Contractors are eligible to receive certification at one of three maturity levels, each with its own set of cyber security requirements. The appropriate level will be determined based on the contract the organization is looking to obtain.

Shared Accountability: CMMC certification requires a coordinated effort on behalf of all parties that handle confidential information belonging to the DOD. Prime contractors are required to ensure that the subcontractors they outsource work to are fully aware of the CMMC-related components of a given contract. Furthermore, prime contractors bear the responsibility of verifying the security measures implemented by their subcontracting partners.

CMMC Costs: The total cost of CMMC certification will vary by a wide range of factors. These variables may include the size and complexity of the IT infrastructure, the maturity of the security mechanisms deployed to safeguard the infrastructure, and the scope and volume of the data the contractor has in their possession. According to the DOD, associated costs will be affordable and align with the desired certification level.

> ***CMMC IS POISED TO HAVE MAJOR IMPLICATIONS FOR COMPANIES ACROSS MULTIPLE INDUSTRIAL VERTICALS.***

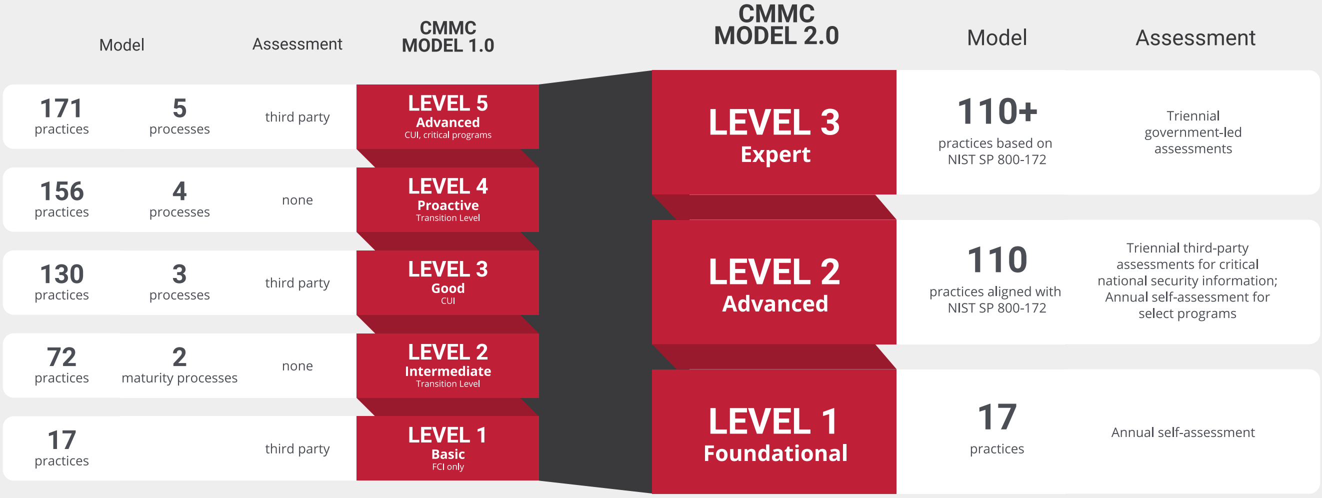
Ramifications: The repercussions of failing to meet CMMC compliance are crystal clear — follow the certification guidelines, or lose the privilege to view, compete for, and secure contracts with the Department of Defense. While no fines or penalties have been specified, breaching an existing DOD contract could potentially result in monetary damages or other severe consequences.

CMMC COMPLIANCE CHALLENGES

Navigating the many layers of security compliance is often a tedious and time-intensive endeavor. The CMMC framework is no exception. In addition to implementing a number of cyber security technologies, companies are required to produce documentation pertaining to adoption plans, various IT management processes, and personnel policies during the audit. Small and medium-sized firms, especially, may find it incredibly challenging to deploy the resources necessary to meet the rigid demands of CMMC.

As is the case with any new compliance program, the most pressing challenges CMMC pose relate to the lack of awareness surrounding the framework. This is due in large part to the fact that some of the guidelines have yet to be defined. On a positive note, there are plenty of resources in the form of existing cyber security frameworks and training tools available to help contractors prepare for the assessment. It is up to certification-seeking firms to devise a top-down game plan that prioritizes CMMC awareness, and ultimately fosters a culture of compliance across the organization.

SECTION 3
CMMC TIERS EXPLAINED



Model		Assessment	CMMC MODEL 1.0
171 practices	5 processes	third party	LEVEL 5 Advanced CUI, critical programs
156 practices	4 processes	none	LEVEL 4 Proactive Transition Level
130 practices	3 processes	third party	LEVEL 3 Good CUI
72 practices	2 maturity processes	none	LEVEL 2 Intermediate Transition Level
17 practices		third party	LEVEL 1 Basic FCI only

CMMC MODEL 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-172	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

CMMC model 1.0 has been replaced with CMMC model 2.0

LEVEL 1
FOUNDATIONAL

The most notable change CMMC 2.0 brings to the forefront is removal of the mandate that calls for contractors to pass third-party audits at each level in order to obtain certification. Per the updates, Level 1 will now require self-assessments, to be performed on an annual basis, in addition to affirmation that the contractor has uploaded the results to the Supplier Performance Risk System (SPRS), the web-based portal the DOD uses to identify, monitor, and analyze the outcomes of self-reported assessments.

Level 1 also requires the implementation of 17 security measures adopted from NIST SP 800-171. These standards are considered basic requisites of protecting DIB IT systems.

LEVEL 2
ADVANCED

Prior to CMMC 2.0, level 2 was largely viewed as a means of transitioning to the the next maturity level. As such, level 3 is now essentially level 2. This tier requires contractors to implement 110 security measures from NIST SP 800-171 and follow the level 1 mandate of submitting annual self-assessment results to the SPRS. However, companies that handle critical government data pertaining to national security will be required to undergo a C3PAO audit every three years.

LEVEL 3
EXPERT

Absorption into level 2 has rendered the third CMMC tier a work in progress. The final requirements will be announced at a later date. What has been established is the mandatory adoption of roughly 110 NIST SP 800-171 controls as well as additional standards from various other compliance programs. More importantly, level 3 assessments will be performed by the government, rather than a C3PAO.

As the most demanding tier, Level 3 places an enhanced focus on planning and documentation. Contractors will be required to produce a plan that demonstrates their understanding of the necessary security controls. This may include details pertaining to data handling procedures, employee training programs, risk mitigation, and backup schedules among other details.

CMMC LEVELS AND DESCRIPTIONS

MODEL		ASSESSMENT
110+ practices based on NIST SP 800-172	03	Triennial government-led assessments
110 practices aligned with NIST SP 800-172	02	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
17 practices	01	Annual self-assessment

CMMC LEVEL EXCEPTIONS

While the tiered system remains a vital cog in the CMMC certification machine, there are exceptions to the established rules. For instance, select contractors may be eligible to obtain a waiver that allows them to forgo certification requirements at any level. These waivers must be approved by DOD management and are valid for a predetermined length of time.

CMMC 2.0 will also grant companies a sort of grace period to certify at their desired level. This extension is limited to scenarios where undergoing the assessment process could potentially compromise mission-critical operations.

GET ON THE LEVEL

The DOD has made a concerted effort to streamline the CMMC compliance program. With that said, the path to certification will likely be a time-consuming process that demands the utmost preparation and attention to detail. Understanding how the level requirements impact your organization is a crucial step along the potentially long road ahead.

SECTION 4
CMMC CERTIFICATION REQUIREMENTS

Self-assessment has long been a staple of regulatory compliance programs. Companies take the initiative to review and audit the systems and procedures they are responsible for, and then forward the results to the regulatory body overseeing the program. The problem with this model lies in the fact that not all parties applying for certification can be trusted to accurately report the nature of those assessments. Moreover, even applicants who are 100 percent honest may underestimate the importance or complexity of the processes necessary to achieve true compliance.

To preserve the integrity of the cyber security infrastructure across the collective DIB, the DOD has implemented a compliance framework that requires certification via CMMC third-party assessment organizations (C3PAOs). Accredited by the CMMC Accreditation Body (CMMC-AB), which operates independent of the US government, these organizations perform on-site assessments that demonstrate whether a given contractor has met the requirements necessary to achieve certification based on the rules defined by the CMMC compliance model.

C3PAO

C3PAO - INDEPENDENT ORGANIZATIONS THAT PERFORM ON-SITE ASSESSMENTS OF CONTRACTORS TO HELP DETERMINE COMPLIANCE LEVELS.

ANALYZING THE ASSESSMENT PROCESS

CMMC assessment involves a thorough evaluation of the mechanisms implemented to safeguard sensitive data. These assessments will specifically target controlled unclassified information (CUI). Any other information, even data sets protected under compliance frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) or Trade Agreement Act (TAA), is of little relevance. The importance of such information will ultimately be defined by its alignment with CMMC certification.

While the specifics of the auditing process have yet to be revealed, our familiarity with regulatory compliance programs across the cyber security landscape gives us an idea of what CMMC assessment should look like.

ASSESSMENT OF THE IT INFRASTRUCTURE

In most cases, the auditor will arrange a meeting with the individual that heads up the company's cyber security operations. Because some firms outsource IT security to third-party specialists, C3PAO officials may review the credentials and responsibilities of the security contact. This initial assessment is performed to validate the individual's level of competence and ability to efficiently manage the infrastructure.

Once the contact's security prowess has been validated, the auditor will perform a comprehensive evaluation of the infrastructure and the scope defined by DOD standards. It is not uncommon for auditors to question various IT components deemed essential to the operation. In the case of CMMC, particular emphasis will be placed on CUI. As such, any system that transmits or stores this information is significant.

CMMC ASSESSMENT INVOLVES A THOROUGH EVALUATION OF THE MECHANISMS IMPLEMENTED TO SAFEGUARD SENSITIVE DATA.

ASSESSMENT OF EXISTING SECURITY PRACTICES

One of the most important aspects of the auditing process is a thorough evaluation of the security mechanisms currently in place. The objective here is determining whether the company has taken the measures to protect the CUI covered by CMMC. Depending on the contractor's level of preparedness, the security officer may be informed that significant changes are required. The slightest inconsistency could be considered a hole that renders the infrastructure vulnerable to security threats.

PROCESS VALIDATION

Third-party auditors must confirm that the security measures specified have been properly implemented. How this analysis is conducted will be determined by the company's desired CMMC level, as well as the security control under evaluation. For example, the auditor may request to review a company-wide password policy across protected databases.

In the case of technical processes, a hands-on demonstration may be required to illustrate the capabilities of the systems that facilitate those specific functions. The inability to produce viable evidence could result in violations, or even legal repercussions should the action be deemed dishonest, or a purposeful misrepresentation of the implementation in question.

AUDIT REPORT

After conducting an extensive review of the security environment, the auditor will issue a documented report of the findings. In determining the company's level of compliance, the report will highlight performance in each assessment area. Keep in mind that any noted issues does not guarantee a failed audit. In fact, it is fairly common for audits to yield faults, particularly when new standards are introduced. Most assessments offer a threshold of allowable failure, which is typically based on whether the fault compromises protected data.

Acing the CMMC assessment is a big win for those seeking certification — but not an invitation to relax. Per the DOD, the framework is an evolving standard that will likely demand considerable modifications as new security threats emerge. With a clear understanding of the process, contractors can make preparations that greatly improve their prospects of obtaining that coveted certification.

SECTION 5

CMMC AUDIT PREPARATIONS

CMMC is one of the most important compliance standards to come along in the modern digital age. One could argue that is among the most complex as well. The DOD is demanding contractors to endure a rigid assessment process that technically, has never been conducted before. What's more, CMMC is very much a work in process. Some of the specifics are currently being formalized in the federal rulemaking process, while training courses are being provided to ensure the program can field a serviceable number of assessment and certification professionals.

THE DOD IS DEMANDING CONTRACTORS TO ENDURE A RIGID ASSESSMENT PROCESS THAT TECHNICALLY, HAS NEVER BEEN CONDUCTED BEFORE.

The book on CMMC is still being written. That said, optimal preparation is invaluable. This section will cover the groundwork to make sure you're ready for the audit process.

TEND TO YOUR DATA ENVIRONMENT

The first task on the agenda is taking an exhaustive look at your IT environment. You need to determine which sets of data are relevant to the CMMC scope, as well as the systems responsible for processing, transmitting, and storing that information. The protected data or CUI, covers a broad range of information, including IT assets related to the following areas:

- Campaign funds
- Criminal records
- Electronic funds transfers
- Federal tax payers
- Foreign intelligence
- Physical security operations
- Patent applications

While CMMC prioritizes confidential information in non-government systems, contractors may possess data that intersects with existing government data at various points across their infrastructure. Careful analysis of your environment will go a long way in setting the tone for a relatively clean audit procedure.

FOLLOW ESTABLISHED ROADMAPS

There is no single silver bullet to ensure impenetrable cyber security. As such, guidelines tend to share characteristics from one compliance standard to the next. Contractors targeting CMMC certification would be wise to consider how and what they can borrow from existing compliance standards. The most obvious example is the framework CMMC is designed to usurp — NIST SP 800-171. Although the standard left plenty to be desired in the way of uniformity, NIST SP 800-171 provides specific guidelines for handling CUI in non-government systems, which is the basis of CMMC.

Implementing security measures culled from NIST SP 800-171 or other regulatory standards will not guarantee CMMC compliance. However, the practices preached in those programs may very well ease the transition along the road to certification. Take the time to review any existing compliance programs with potentially reciprocal criteria. At the very least, the knowledge gleaned from those assessments can give you a better understanding of the CMMC auditing process.

ASSESS YOUR PREPAREDNESS

Considering the sensitivity of government business, there's a great chance that DOD contractors have already implemented many of the essential security measures CMMC certification requires. Nevertheless, it's vital to understand your level of preparedness before heading into an audit.

An internal evaluation should assess your readiness in the following areas:

Roles and responsibilities: Who manages IT security in your organization? Is senior management involved in the process? If so, to what degree? How often does IT security personnel assess your level of risk?

IT security: How does your IT security team monitor the network to detect and remediate potential vulnerabilities? What controls have been implemented to protect the environment in the event that threats are detected?

Access control: Who has access to CUI across your organization? What measures have been taken to prevent unauthorized access to that data and the systems that house it?

Partner relationships: How do vendor relationships potentially impact your compliance status? Are those partners accounted for in your risk assessment strategy?

Business continuity: Is your company equipped to recover from a security incident or natural disaster? How often is that response plan tested?

Training and education: Does staff understand the security measures implemented to protect the network? Are they actually following the protocols and procedures set in place?

The process of accessing your preparedness should be as extensive as the audit for CMMC certification. Due to the detailed nature it demands, it is advisable to consider bringing in a third-party firm to perform an assessment of the IT environment. An impartial evaluation will help to ensure that you're ready for the official audit by providing an honest assessment of your cyber security prowess.

AN INTERNAL EVALUATION SHOULD ASSESS YOUR READINESS IN THE FOLLOWING AREAS:

01 ROLES AND RESPONSIBILITIES

02 IT SECURITY

03 ACCESS CONTROL

04 PARTNER RELATIONSHIPS

05 BUSINESS CONTINUITY

06 TRAINING AND EDUCATION

ADDRESS IDENTIFIED PROBLEMS

The cyber security threat landscape is constantly evolving. Systems that are secure today, might be outdated and vulnerable to new attacks tomorrow. If the assessment yields problem areas that warrant attention, initiative must be taken to remediate them and bring the organization closer to compliance. Filling security holes often calls for additional investments, so it makes sense to estimate what it will cost to address each gap uncovered in the assessment.

Although the cost of CMMC audits may be redeemable after receiving certification and subsequent contract awards, the same cannot be said for the resources you shell out to get there. Consider it money well spent. This is now the price of doing business with the Defense Department, and the cost of non-compliance is more than any contractor is willing to wager.

NO TIME LIKE THE PRESENT

Recognizing the challenge at hand, the DOD introduced CMMC as a five-year rollout that would give contractors ample time to adapt to the program. Organizations can stay ahead of the curve by making audit preparations as soon as possible. This proactive approach will better assure that you are compliant well before the final deadline rolls around.

CMMC: FURTHER READING

This next section will help you navigate the vast and complex world of CMMC compliance. We will overview the key terms, answer some of the most frequently asked questions about the framework, and provide access to resources that are sure to make a valuable addition to your CMMC toolkit.

SECTION 6
CMMC GLOSSARY

Controlled unclassified information (CUI)
Data that requires protection or specific security measures according to regulations defined by federal policies. CUI may exist in the following categories:

- Critical infrastructure
- Financial services
- Immigration
- Intelligence
- Law enforcement
- National defense
- Natural resources
- Nuclear weapons
- Statistical analysis

CMMC Accreditation Body (CMMC-AB)
The certification body the US Department of Defense has empowered as the lone authority in the management of CMMC assessments and training procedures.

CMMC Third-party Assessor Organization (C3PAO)
A third-party service provider authorized by the CMMC-AB to facilitate the assessment process for CMMC certification. CMMC certification can only be obtained by passing an audit conducted by an official C3PAO.

Defense industrial base (DIB)
The community of prime contractors and subcontractors that service the Department of Defense.

Contractor
A non-government individual or organization that receives a contract to provide goods or services to the Department of Defense.

Defense Federal Acquisition Regulation Supplement (DFARS)
A set of IT security standards the Department of Defense administers to third-party suppliers. DFARS encompasses specific data handling requirements, product procurement methods, employee policies, and procedures for safeguarding critical information.

Maturity Level
A clearly defined benchmark within an established evolutionary model. In the case of CMMC, each level represents a step in the road to continuous progression.

Maturity Model
A framework or system that charts improvement and progression. This model evaluates an organization's practices, processes, and methodologies against a set of predetermined requirements. In addition to accessing the current degree of effectiveness, a maturity model helps determine what the organization needs to progress to higher tiers within the model.

National Institute of Standards and Technology Special Publication (NIST SP) 800-171
A set of guidelines that dictate how non-government IT systems are to process, transmit, store, and secure controlled unclassified information (CUI). Although CMMC, which is based on many of the same core principals, has been designed to replace it, NIST SP 800-171 compliance is a current requirement for select DOD contracts.

Registered Provider Organization (RPO)
RPOs are authorized by the CMMC-AB to provide consultation and recommendations to clients seeking guidance on CMMC. While they can help organizations prepare for the process, RPOs are not authorized to provide CMMC assessments.

Subcontractor
An individual or organization that works partially or wholly under a primary DOD contractor. Under CMMC, subcontractors are liable to the same rules and regulations mandated to the prime contractors above them.

Supplier Performance Risk System (SPRS)
A software system the DOD uses to house and manage the performance data of its suppliers. A virtual risk assessment platform, the SPRS assigns a risk score to suppliers based on past performance. The DOD takes those results into consideration when awarding contracts valued at $1 million or less.

SECTION 7
CMMC FAQS

How Does CMMC Differ from NIST SP 800-171?

CMMC is based on a tiered model comprised of three levels. Each level contains a set of practices designed to ensure that effective IT security measures are implemented to safeguard CUI. The CMMC framework encompasses the guidelines specified in NIST SP 800-171 as well as cyber security standards from various other compliance programs.

Which Level of Certification is Required for a DOD Contract?

In general, the DOD will determine the appropriate level of CMMC certification based on the contract an organization bids for. The specific level requirements will be furnished when a contractor submits a request for information (RFI) or request for proposal (RFP) for a given contract acquisition.

How is CMMC Certification Obtained?

In order to receive CMMC certification, organizations must undergo an assessment with an authorized C3PAO. Should the organization pass the audit, the C3PAO will issue a certificate in accordance with the targeted CMMC level. The certificate and the results of the audit will be forwarded to the DOD, essentially granting the company contract eligibility.

What is the Cost of CMMC Certification?

The amount a contractor pays for CMMC certification is dependent on a number of factors. The desired level of certification as well as the size and complexity of the company's IT network is among the variables that will be considered.

What About Recertification?

CMMC certifications are generally based on a triennial lifecycle. As it stands, contractors will need to undergo reassessment every three years in order to obtain subsequent certification.

How Long Do I Have?

The DOD has targeted October 1, 2025 as the final deadline for CMMC compliance. From there, certification will be required to obtain any contracted work with the DOD. The amount of preparation required may vary greatly depending on the contract, so time is of the essence.

Are There Any Exceptions?

CMMC compliance does not apply to contractors that specialize in commercial off-the-shelf (COTS) offerings. Exclusively applicable to hardware and software programs, COTS is defined by three characteristics:

1. Distribution in large quantities on the commercial marketplace
2. Typically used by the general public or commercial entities for non-government applications
3. Made available to government entities without alterations

SECTION 8
CMMC RESOURCES

OUSD Acquisition & Sustainment
The designated portal for the CMMC framework, this website provides extensive details on the model, the changes introduced in version 2.0, assessments, and implementation.

CMMC Accreditation Body
The CMMC AB portal is a centralized hub dedicated to the essential third-party component of CMMC. This website is a prime resource for prospective C3PAOs, individual auditors, and other entities that wish to obtain the credentials to aid the certification process.

National Archives and Records Administration
This section of the National Archives website serves as a knowledge base for CUI. Here you'll find a searchable CUI database, training tools, and other resources dedicated to controlled unclassified information.

Center For Development of Security Excellence
A centralized educational hub that provides a collection of training resources for DOD contractors, personnel, and members employed by other government agencies. The website features various learning tools and courses designed to highlight established DOD security principals.

Security Awareness Hub – Insider Threats
An online training course designed to identify and report activities that indicate threats originating from within the organization.

DATALOCKER®

DATALOCKER
+1 913-310-9088

sales@datalocker.com
To find your local DataLocker Reseller please visit
datalocker.com