THE CMMC 2.0 CHECKLIST

YOUR COMPANY'S ROADMAP TO COMPLIANCE

TestPros™

WWW.TESTPROS.COM

TABLE OF CONTENTS

As a defense contractor, achieving and maintaining CMMC compliance is vital for securing contracts with the Department of Defense (DoD). This guide lays out a step-by-step roadmap to help your company navigate the Cybersecurity Maturity Model Certification (CMMC) process.

Q What is CMMC?

→ The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity program spanning across all defense industrial base (DIB) partners. The U.S. Department of Defense (DoD) mandates CMMC compliance for all its contractors and subcontractors.

The latest CMMC framework (v2.0) establishes three security maturity levels that organizations must adhere to. The DoD uses these levels to determine when issuing Requests for Proposals (RFPs) and selecting vendors.

Q When is CMMC compliance required?

→ CMMC 2.0 was introduced in November 2021. However, the official program pilot phase and implementation experienced delays, leading to ongoing program changes and requirements.

The regulatory process to update the DFARS-7012 requirements is also pending, causing further delays in incorporating CMMC requirements into RFPs.

Despite the setbacks, organizations should be prepared for full CMMC implementation which is expected in 2023. Non-compliant contractors may risk losing access to DoD contracts.

Q Who needs to be CMMC certified?

→ CMMC applies to all organizations within the defense industrial base (DIB). This includes over 300,000 prime contractors, subcontractors, universities, researchers, engineers, and supply chain staff involved in producing equipment and/or providing services for the U.S. Armed Forces.

Q What is needed for CMMC compliance?

→ DIB manufacturers must ensure that their enterprise network or parts of it handling sensitive information meet certain security standards to comply with the CMMC rules. They should also ensure that all networks that can communicate with each other or be used for stealing data have the same security measures in place.

While some organizations possess the necessary staff, resources, and expertise to meet CMMC requirements internally, many will require external assistance to achieve and maintain compliance.

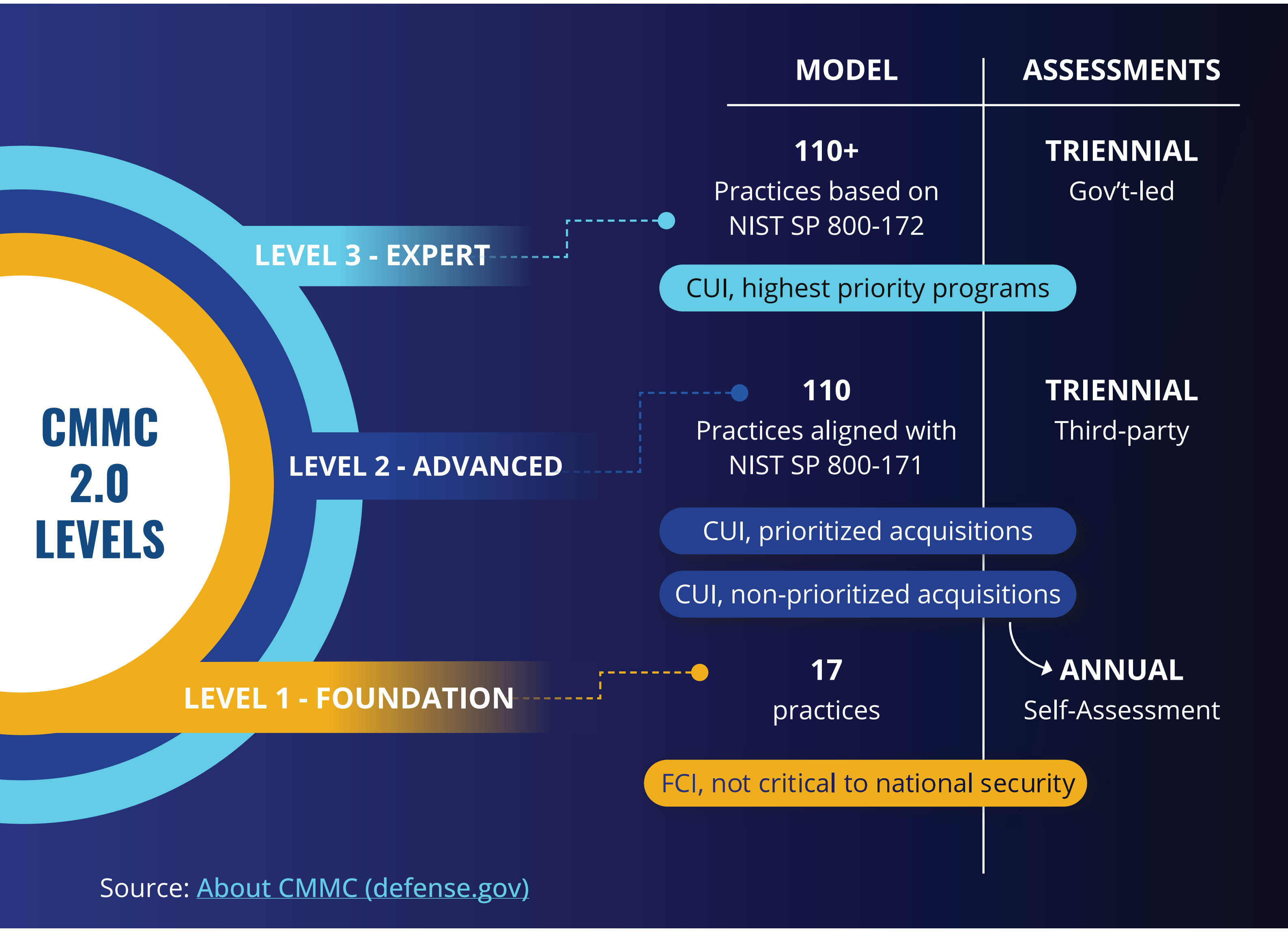
Q What are the CMMC 2.0 requirements?

→ Organization's must implement certain cybersecurity practices stemming from 14 domains. Each CMMC level requires more practices from these domains.

1. ACCESS CONTROL (AC)
2. IDENTIFICATION AND AUTHENTICATION (IA)
3. PERSONNEL SECURITY (PS)
4. SYSTEM AND COMMUNICATIONS PRTECTION (SC)
5. AWARENESS AND TRAINING (AT)
6. INCIDENT RESPONSE (IR)
7. PHYSICAL PROTECTION (PE)
8. SYSTEM AND INFORMATION INTEGRITY (SI)
9. AUDIT AND ACCOUNTABILITY (AU)
10. MAINTENANCE (MA)
11. RISK ASSESSMENT (RA)
12. CONFIGURATION MANAGEMENT (CM)
13. MEDIA PROTECTION (MP)
14. SECURITY ASSESSMENT (CA)

Q What are the levels of CMMC?

→ Three compliance levels represent varying degrees of cybersecurity maturity that DoD contractors must adhere to, depending on the type of information they handle. The CMMC 2.0 levels are:



	MODEL	ASSESSMENTS
LEVEL 3 - EXPERT	**110+** Practices based on NIST SP 800-172 CUI, highest priority programs	**TRIENNIAL** Gov't-led
LEVEL 2 - ADVANCED	**110** Practices aligned with NIST SP 800-171 CUI, prioritized acquisitions CUI, non-prioritized acquisitions	**TRIENNIAL** Third-party
LEVEL 1 - FOUNDATION	**17** practices FCI, not critical to national security	**ANNUAL** Self-Assessment

Source: About CMMC (defense.gov)

Level 1: Foundational

- Applicable to contractors who manage Federal Contract Information (FCI), not Controlled Unclassified Information (CUI)
- Ensures basic cybersecurity practices are in place, protecting FCI from unauthorized access and disclosure.
- The third-party assessment is generally not required, allowing for annual self-assessments and attestation of compliance.
- Scoping Guidance - Level 1
- Self-Assessment Guide - Level 1
- Level 1 contains 17 practices stemming from FAR Clause 52.204-21

ACCESS CONTROL (AC)	IDENTIFICATION AND AUTHENTICATION (IA)	MEDIA PROTECTION (MP)
• AC.L1-3.1.1 – Authorized Access Control • AC.L1-3.1.2 – Transaction & Function Control • AC.L1-3.1.20 – External Connections • AC.L1-3.1.22 – Control Public Information	• IA.L1-3.5.1 – Identification • IA.L1-3.5.2 – Authentication	• MP.L1-3.8.3 – Media Disposal
PHYSICAL PROTECTION (PE)	**SYSTEM AND COMMUNICATION PROTECTION (SC)**	**SYSTEM AND INFORMATION INTEGRITY (SI)**
• PE.L1-3.10.1 – Limit Physical Access • PE.L1-3.10.3 – Escort Visitors • PE.L1-3.10.4 – Physical Access Logs • PE.L1-3.10.5 – Manage Physical Access	• SC.L1-3.13.1 – Boundary Protection • SC.L1-3.13.5 – Public-Access System Separation	• SI.L1-3.14.1 – Flaw Remediation • SI.L1-3.14.2 – Malicious Code Proection • SI.L1-3.14.4 – Update Malicious Code Protection • SI.L1-3.14.5 – System & File Scanning

Level 2: Advanced

- Targeted at contractors who handle CUI, requiring more stringent security measures.
- Builds upon the foundational practices of Level 1 by implementing additional security controls to safeguard CUI.
- In most cases, a third-party assessment is required every three years to validate the proper implementation of security practices.
- Level 2 contains 110 practices aligned with NIST SP 800-171
- Scoping Guidance - Level 2
- Self-Assessment Guide - Level 2

Level 3: Expert

- A specialized cybersecurity maturity level relevant for only a small subset of defense contractors.
- Demands the highest degree of security measures to protect highly sensitive information and systems.
- Ensures the contractor can thwart advanced persistent threats (APTs) and maintain robust cybersecurity practices.
- Requires a government-led assessment every three years.
- Level 3 contains 110+ practices based on a subset of NIST SP 800-172

CMMC COMPLIANCE CHECKLIST: A SIX-PHASE OVERVIEW

Whether you're a small business or a large corporation, this checklist provides the information and resources needed to achieve compliance. Follow the steps in order as you navigate the certification process.

Need assistance or have questions? Leave a comment below or reach out to our team of experts by clicking here.

Phase 1: Scoping (Getting Started / Requirements Analysis)

In this initial phase, your goal is to determine your CMMC level by identifying Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) in your environment. This is crucial for understanding the specific requirements your organization needs to meet.

Key steps in this phase include:

Determine your CMMC level: Each level has a specific set of controls, with Level 1 being the most basic and Level 3 being the most advanced. As you progress to higher levels, more security controls and practices are added. Your level is determined by the type of CUI you store and process. For instance, if you handle Level 3 CUI, you must implement Level 3 controls. Check the DoD's Scoping Guidance for Level 1 and Level 2 for more information.

Review the NIST SP 800-171 DoD Assessment (scoring) Methodology (DAM): This assessment methodology provides a standardized approach to evaluating your organization's implementation of the security requirements found in NIST SP 800-171. By familiarizing yourself with this methodology, you can better understand the expectations and requirements for achieving CMMC certification.

Identify the people, processes, and technology applied to your DoD contract(s): Whether you currently have a DoD contract or are bidding on one, you must understand the various components involved. This includes the personnel responsible for handling sensitive information, the processes in place to protect that information, and the technology used to store, process, and transmit data. Check your level's scoping guidance for more information.

Collaborate with internal teams (Information Security, Legal, HR, Finance) to understand each department's role in CMMC compliance. This may involve developing interdepartmental communication channels and coordinating efforts to ensure a unified approach to compliance.

Document subcontractors and external service providers: Understand that CMMC requirements extend beyond your organization. If subcontractors and external service providers come into contact with CUI, the same requirements are imposed on them, and they must be compliant at the same level as your organization.

Phase 2: Planning (Scope Assessment Boundary / Data Gathering)

Get your documentation in order during Phase 2. Focus on taking inventory, drafting a SSP, and selecting required security controls based on your CMMC level. If you need help, seek professional guidance from a CMMC Consultant or a Registered Practitioner Organization (RPO). Otherwise, follow these steps:

Create an Asset Inventory: Identify and list all system and data assets that interact with CUI. Your asset inventory should include hardware, software, data storage components, and any cloud-based services your organization uses. By comprehensively understanding your assets, you can better protect your sensitive information and comply with requirements.

Draft a System Security Plan (SSP): The SSP document outlines your organization's security policies, procedures, and controls. It should describe how your organization meets the requirements and provide a detailed roadmap for maintaining compliance. The SSP should be regularly reviewed and updated as necessary to reflect changes in your organization's security posture. Download NIST.gov's SSP Template here. Complete this and print it out for an auditor

Develop a Network Diagram to define the System Boundary: The network diagram should illustrate your organization's IT infrastructure and show how data flows within and outside your network. By defining the system boundary, you can identify areas where CUI is stored, processed, or transmitted and prioritize the implementation of security controls.

Select required security controls based on your CMMC level: Each CMMC level requires a specific set of security controls and practices. Based on your organization's CMMC level, identify the controls and practices you need to implement. Find the required practices described for Level 1, Level 2 and Level 3.

Create a Plan of Actions & Milestones (POA&M) Template to be completed after an audit: The POA&M document tracks the progress of your organization's security improvements. The template should include a list of deficiencies identified during the audit, the corresponding corrective actions, and expected completion dates. The POA&M will be updated as a living document to reflect your organization's progress toward CMMC compliance. Download NIST.gov's POA&M template here.

Phase 3: Assessment (Internal/External Assessment)

It's time to prepare for an assessment. In Phase 3 you will evaluate your organization's security posture against the CMMC requirements and determine where you stand.

Perform an assessment using the SSP: Evaluate your organization's implementation of the required security controls and practices. This assessment should be conducted by qualified personnel, either internal staff or external consultants, depending on your organization's resources and expertise. You can use the DoD's Self-Assessment Guide for Level 1 and Level 2.

Document assessment results in a Security Assessment Report (SAR): The SAR details the findings of your assessment, including any deficiencies identified and recommendations for improvement. Document your assessment results by adding your findings in the SSP document.

Identify any deficient CMMC practices in the POA&M: Review the SAR and update the POA&M with any identified deficiencies. This will help your organization track its progress toward compliance and prioritize remediation efforts.

Complete the DFARS Compliance Checklist: The Defense Federal Acquisition Regulation Supplement (DFARS) outlines specific cybersecurity requirements for contractors working with the DoD. Ensure your organization meets these requirements by completing the DFARS Compliance Checklist.

Upload the three artifacts (SSP, SAR, and POA&M) to the Supplier Performance Risk System (SPRS): The SPRS serves as a repository for your organization's CMMC compliance documentation. You demonstrate your commitment to achieving and maintaining compliance by uploading these artifacts. [Access the SPRS here]

Submit your self-assessment score to SPRS: Your organization's self-assessment score reflects its current security posture. Submitting this score to SPRS provides the DoD with valuable information about your organization's progress toward CMMC compliance.

Phase 4: Remediate Remaining Risks

Take your assessment results and make improvements. Fix (remediate) what's left, then update your documents for the certification stage in Phase 5

Remediate risks: Use the POA&M as a guide and implement the remaining CMMC controls/practices. The objective is to achieve a clean POA&M.

Update the POA&M, SSP, SAR, and DFARS Compliance Checklist: Resubmit updated artifacts into SPRS, generating an updated score.

Phase 5: Certified CMMC Assessment via CMMC C3PAO

As an Organization Seeking Certification (OSC), in this phase you must engage with a CMMC 3rd Party Assessment Organization (C3PAO) to scope and contract for an independent assessment. Follow these steps:

Coordinate and plan the CMMC assessment with the C3PAO: Engage with the C3PAO to discuss your organization's readiness for the assessment and establish a mutually agreeable timeline.

The C3PAO conducts an independent assessment to verify compliance with the CMMC 2.0 maturity level (1 through 3, as applicable): The C3PAO's assessment will validate your organization's implementation of the required security controls and practices, as well as its overall security posture.

The C3PAO issues independent reports to the OSC and uploads the assessment report into CMMC EMASS, which the DoD can access: Once the CMMC assessment is complete, the C3PAO will provide your organization with a detailed report outlining its findings. This report will also be uploaded to the CMMC Enterprise Mission Assurance Support Service (EMASS) system, making it accessible to the DoD for review and decision-making.

Support the DoD Joint Surveillance Assessment, which can provide a competitive advantage when securing DoD contracts: Volunteering for this assessment demonstrates your commitment to maintaining a high level of cybersecurity. Participating in the Joint Surveillance Assessment showcases your organization's dedication to continuous improvement and may gain a competitive edge in procurement.

Phase 6: Maintain & Monitor Compliance

Congratulations! You're now certified for CMMC 2.0. In the final phase, focus on maintaining and monitoring your CMMC compliance by following these last steps:

Implement continuous procedures for updating training, processes, and related artifacts: CMMC compliance requires regular updates to training materials, security processes, and documentation. Establish a schedule for reviewing and updating these items to ensure your organization complies with the evolving cybersecurity landscape.

Execute assessments and submit updated artifacts into SPRS and CMMC EMASS, either through your organization or a C3PAO, as applicable: Regular assessments are critical for maintaining CMMC compliance. Whether conducted internally or through a C3PAO, these assessments help identify areas for improvement and ensure that your organization's security posture aligns with compliance requirements.

TAKE CHARGE OF YOUR CMMC COMPLIANCE WITH TESTPROS

At TestPros, we specialize in compliance and understand its significance. While we do use automation, we do not solely rely on it. Our unique approach involves thorough manual validation to ensure your company's compliance. With decades of experience, we have helped countless organizations secure government contracts.

If you're seeking professional assistance in achieving CMMC certification, our team of experts is ready to guide you through the entire process, including gap analysis, readiness assessment, remediation, and certification.

Do not risk your organization's security and future opportunities. Choose TestPros for a secure future in the defense industry.

WHAT NEXT?

Contact us – Let us know what questions you have. Begin your CMMC certification journey today.

Book an introduction call – Speak with one of our CMMC specialists at your convenience.

Company Headquarters - 46090 Lake Center Plaza # 306, Sterling, VA 20165

Company Phone# (703) 787-7600

FAQs

Q What does it mean to be CMMC compliant?

Being CMMC compliant means that your organization has successfully implemented the required cybersecurity practices and processes outlined by the Cybersecurity Maturity Model Certification (CMMC) for your designated maturity level. This involves ensuring adequate security measures are in place to protect sensitive information and demonstrating adherence to the CMMC framework during a third-party assessment.

Q How can my organization achieve CMMC certification?

To achieve CMMC certification, your organization needs to follow these steps:

- Determine the required CMMC level for your organization based on the type of information you handle.
- Perform a gap analysis and readiness assessment to identify areas needing improvement.
- Remediate any identified gaps and implement required security practices and processes.
- Schedule a third-party assessment with a CMMC Third-Party Assessment Organization (C3PAO).
- Successfully pass the third-party assessment and receive your CMMC certification.

Q How often do I need to renew my CMMC certification?

Level 1 organizations who self-certify must do so on an annual basis. Level 2 organizations who work with a C3PAO have their certification valid for three years. After this period, your organization must undergo another third-party assessment to renew your certification and demonstrate continued compliance with the CMMC requirements.

Q What happens if my organization is not CMMC compliant?

If your organization is not compliant, you risk losing eligibility for new DoD contracts or even having existing contracts terminated. It is essential to work towards achieving and maintaining CMMC compliance to remain competitive in the defense contracting landscape and protect your organization’s sensitive information.

Q When did CMMC start?

The initial CMMC framework was released in January 2020. A Memorandum of Understanding (MOU) between the DoD and the CMMC Accreditation Body was signed, and certification, licensing, and training requirements for assessors and organizations were put in place.

CMMC 2.0 was introduced in November 2021. Find both versions available on the DoD CMMC website.

Q How can I control internal system access to ensure CMMC compliance?

Controlling internal system access is critical for CMMC compliance. Here are some ways to achieve this:

- Implement strong access control policies to limit user access based on their role and need-to-know basis.
- Establish proper authentication and authorization processes, such as multi-factor authentication and secure password policies.
- Regularly review and audit user access rights and permissions.
- Provide cybersecurity training and awareness programs for employees to reinforce the importance of following access control policies.