teal

Advanced CMMC Guide and Compliance Checklist

Fortify Your Business Against Cybercrime

Introduction

The Defense Supply Chain (DSC) faces a growing number of cyber threats from nation-states and non-state actors. The need for a higher level of protection prompted the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) to develop the Cybersecurity Maturity Model Certification (CMMC). This model aims to standardize cybersecurity practices and introduce a new audit process for ensuring compliance.

However, Department of Defense (DoD) contractors and subcontractors may find the compliance process overwhelming. To successfully navigate CMMC, companies must take extra precautions and ensure they thoroughly understand the requirements. Use this guide to help your company prepare for your upcoming CMMC certification.

This guide includes:

- The purpose of CMMC
- Benefits of CMMC compliance
- An overview of the process
- CMMC maturity levels
- A pre-assessment compliance checklist
- How to prepare for your CMMC audit
- How Managed IT Services Help DoD Contractors

The Purpose of CMMC

The DoD introduced the CMMC certification framework in January 2020 to enhance the cybersecurity of the US Defense Industrial Base, which consists of over 300,000 companies. This framework ensures that private sector defense contractors and subcontractors comply with cybersecurity standards to safeguard Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).

On November 4, 2021, the DoD formally announced what is commonly referred to as CMMC 2.0 – which has an updated program structure and requirements. This new model aligns cybersecurity requirements to other federal requirements.

Previously, contractors were responsible for securing their IT systems and safeguarding any confidential DoD information stored or transmitted on them. While contractors are still ultimately responsible for adhering to cybersecurity requirements, the CMMC framework adds an extra layer of scrutiny by mandating third-party assessment and verification to evaluate the organization's security posture.

Benefits of CMMC Compliance

This compliance framework is essential to your organization's cybersecurity as you support the DoD in its mission. The benefits of CMMC are plentiful and include:

- Maximizing cybersecurity resilience.
- Recovery from cyber-attacks without financial consequences.
- Utilizing cybersecurity best practices across maturity levels.

The updated model is also beneficial for small businesses as it helps reduce costs – which is a big win for companies that have a limited budget.

Do I need to be certified?

You need to be CMMC certified if you:

- □ Engage with the DoD or a contractor working for the DoD.
- □ Are a member of the DoD's Defense Industrial Base supply chain.
- □ Are a subcontractor under a prime contractor whose prime contractor communicated that you must meet a specific maturity level.

Every contract outlines the required CMMC maturity level for the DoD supplier and its subcontractors before receiving the contract. It is the responsibility of the prime contractors to verify that all subcontractors meet the required maturity level.

How does the certification process work?

To ensure the security of sensitive information, DIB contractors must obtain a third-party certification from a C3PAO under the CMMC mandate. The Cyber Accreditation Body (CyberAB) was created as an independent organization that authorizes and accredits the CMMC Third Party Assessment Organizations (C3PAOs).

Level 1 Self-certification

Level 1 certification allows for self-certification, but with the CMMC Assessment Guides now available from the DoD, businesses can conduct an initial self-assessment. However, many organizations prefer to partner with sophisticated organizations, like Teal, to ensure a seamless and successful process.

Level 2 & 3 Formal Certification

To receive a formal certification, companies must choose an authorized or accredited C3PAO from the CyberAB Marketplace. Once selected, you will go through the following four steps:

1. You and your C3PAO collaborate on the CMMC assessment.
2. The C3PAO delivers an assessment report to CyberAB for review.
3. CyberAB reviews the assessment for successful completion.
4. If CyberAB is confident that it was successful, it issues the appropriate certificate and submits a copy of everything to the DoD.

How a Registered Provider Organization (RPO) Can Prepare You

It is crucial to clearly understand the maturity levels outlined by CMMC to determine the appropriate level for your organization. As a Registered Provider Organization (RPO), Teal’s Registered Practitioners (RPs) provide advanced implementation services. Their expertise can help your organization meet CMMC practices and assist in creating the required documentation.

Teal's RPs provide a comprehensive solution that helps you ace your certification assessment. Our team of experts perform readiness assessments based on people, processes, and technology to evaluate your current security program using a proven methodology. Our team's sophisticated expertise provides you with actionable recommendations to ensure you meet your desired CMMC maturity level.

The CMMC Maturity Levels

The CMMC framework consists of three maturity tiers that reflect the depth of an organization's security program implementation. These tiers are aligned with best practices and processes mapped across domains, ranging from foundational to expert levels, which are related to the type of DoD or US government data an organization interacts with.

As the framework is cumulative, earlier levels' requirements must be met for the desired certification level. Understanding the necessary maturity levels and capabilities needed for each level is crucial for successful DoD collaboration.

The DoD strives to ensure that CMMC implementation is affordable – even for small businesses - to promote secure engagements even at the lower CMMC levels.

MATURITY LEVEL	DESCRIPTION
Level 1 – Foundational Cyber Hygiene	Performs in-scope practices.
Level 2 – Advanced Cyber Hygiene	Manages according to documented in-scope practices.
Level 3 – Expert Cyber Hygiene	Optimizes the implementation of in-scope practices.

Level 1: Foundational Cyber Hygiene

This level is designed to ensure that organizations maintain a basic level of cyber hygiene to protect FCI. The specified practices are mandatory, but the assessment of process maturity is not conducted at this level. It's acknowledged that organizations may lack proper documentation and perform practices in an ad-hoc manner.

The 17 Practices that cover the fundamental safeguarding of FCI are spread across 6 Domains and are outlined in 48 CFR 52,204-21 ("Basic Safeguarding of Covered Contractor Information Systems") and NIST SP 800-171.

Level 2: Advanced Cyber Hygiene

Level 2 is a significant step forward in protecting CUI, as it builds upon the foundation of Level 1 expectations. Achieving Level 2 certification requires organizations to document their cyber hygiene processes and implement them - precisely as established.

With 110 Practices spanning 17 Domains and aligned with the NIST SP 800-171 documentation, Level 2 is a crucial transitional step in the journey to safeguarding CUI.

Level 3: Expert Cyber Hygiene

Level 3 certification is an advancement from Levels 1 and 2, with the utmost priority of safeguarding CUI. Organizations must prove that their processes are properly managed to attain Level 3 certification. Accomplishing this entails integrating a comprehensive plan that includes resourcing, training, project plans, and other essential details.

The 110+ Practices mandated in Level 3 are spread across 17 Domains, with 110 Practices from NIST SP 800-171 and a selection of practices from NIST SP 800-172.

CMMC Pre-assessment Compliance Checklist

Before beginning the CMMC assessment process, our experts highly recommend that you thoroughly examine this CMMC compliance checklist. Address gaps in your data, documentation, or practices as soon as possible to ensure you get certified quickly.

1

Determine the CMMC level that your organization needs to obtain.

2

Determine the scope of the data that the assessment will cover.

3

Establish boundaries for how data is managed to put clearly defined limits around the assessment.

4

Review all processes and the level of documentation that exists for each.

5

Fill in any documentation gaps that you identify.

6

Review relevant practices and determine who performs them. Determine if the identified individuals can explain how they perform the tasks.

7

Determine if your organization can conduct these pre-assessment activities or if you will require assistance from an RPO.

CMMC Compliance Checklist

To ace your CMMC assessment, reviewing your organization's capabilities across all 17 Domains associated with the CMMC model is crucial. Look at the checklist below for a high-level overview of what to expect within each Domain and across all three levels.

CMMC DOMAIN	CAPABILITY (SAMPLE)
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post-incident reviews • Test incident response

Preparing for a CMMC assessment is a journey that requires ample time and effort. Our seasoned CMMC experts highly recommend that organizations allocate 12 months for thorough preparation and successful completion of the assessment.

Pre-assessment Process

To successfully undergo a formal CMMC assessment, it is highly recommended for organizations to get a NIST SP 800-171 assessment from a reliable and experienced organization to help them prepare. The CyberAB has a Marketplace which can assist your organization in identifying businesses that have undertaken the prerequisite education and completed the necessary background validation required by the CyberAB to conduct pre-assessment engagements. These organizations are known as Registered Provider Organizations (RPO), or they may be CMMC Third Party Assessment Organizations (C3PAO).

The CyberAB mandates that the organization conducting the final assessment must not have any conflicts of interest with organizations that may have been involved in helping to prepare the business for the final assessment.

Formal Assessment Process

Once an organization is fully prepared for its final assessment, it will collaborate with its chosen C3PAO. The selected entity will then assign a Certified Assessor (CA) to spearhead the assessment. Note: The assessment contract is exclusively between the organization undergoing assessment and the preferred C3PAO.

Certification

After completion of the assessment, the CA will submit their report to their internal review panel for a thorough quality review. Once the internal quality review is successful, the assessment is passed on to the CyberAB for its quality assessment review. A successful review by the CyberAB will lead to issuing a certificate - valid for three years. Note: The certificate is issued only for the specific areas of the organization that were part of the assessment scope and for a particular level of maturity.

How Managed IT Services Help DoD Contractors

Many smaller DoD contractors and subcontractors struggle to address digital security concerns on their own, while larger companies with ample resources and IT personnel have already taken steps to ensure CMMC compliance. Fortunately, managed IT services can provide expert cybersecurity solutions to these contractors.

An MSP that understands the needs of government contractors and the requirements for achieving CMMC certification can conduct a detailed readiness assessment and gap analysis to identify how the contractor’s existing cybersecurity plan needs to be amended to meet certification requirements.

With the MSP's assistance, contractors can develop a comprehensive cybersecurity program that covers everything from intrusion detection and response to advanced endpoint protection and security awareness training. This will ensure ongoing CMMC compliance for the organization.

How Teal Helps Contractors in their Compliance Journey

As a Registered Provider Organization (RPO), Teal's Registered Practitioners (RPs) are well-equipped to provide advanced implementation services that align with CMMC practices. Our Registered Practitioners (RPs) are adept at creating CMMC-required documentation -ensuring that your organization meets all the requirements. Additionally, our RPs can help you prepare for your certification assessment by conducting readiness assessments that evaluate your current security program based on people, processes, and technology, utilizing proven methodology and IT expertise.

The outcome of this assessment will provide you with actionable recommendations that will enable you to achieve your desired CMMC maturity level. Teal offers sophisticated solutions and assistance that are guaranteed to help you successfully prepare for your CMMC certification assessment.

READINESS ASSESSMENTS

Conduct a thorough review of the security program controls to ensure compliance with the necessary CMMC level. Identify any areas where there may be gaps and provide recommendations for remediation to ensure full compliance.

SCOPING DIAGRAMS

Outline where CUI/FCI data is stored, processed, and transmitted.

SYSTEM SECURITY PLAN (SSP) DEVELOPMENT

Assist in creating and updating SSPs.

PLAN OF ACTION AND MILESTONES (POA&M) DEVELOPMENT

Assist with the development and maintenance of POA&Ms.

CMMC PROCESSES DEVELOPMENT

Assistance with the creation of CMMC required processes, including policies, standards, and supplementary documentation.

TECHNICAL IMPLEMENTATION SERVICES

Provide expert architecture and technical project implementation support to facilitate quick and effective remediation activities.

COMPLIANCE MANAGEMENT EXPERTISE

Establish and continuously enhance the requisite governance measures to uphold compliance with CMMC standards.

FRACTIONAL vCISO

Provide ongoing support to maintain compliance with CMMC since adherence is an ongoing obligation and not a singular task.

Empower Your CMMC Journey

By Contacting Us Today

info@tealtech.com

833-FOR-TEAL

Additional Resources for Contractors

➢ CyberAB	➢ Office of the Under Secretary of Defense for Acquisition & Sustainment	➢ Townhalls
➢ Cybersecurity Maturity Model Certification	➢ CMMC FAQs	➢ CMMC Resources