Dewpoint

Bringing Business and Technology Together

COMPLETE

CMMC GUIDE & COMPLIANCE CHECKLIST

PROTECT YOUR BUSINESS FROM CYBERCRIME

dewpoint.com · info@dewpoint.com · 517.316.2860

INTRODUCTION

Navigating Cybersecurity Maturity Model Certification, or CMMC can be daunting for companies of all sizes. In this Complete CMMC Guide and Compliance Checklist, you will find:

- The purpose of the CMMC model
- A detailed overview of the CMMC certification process and the three maturity levels of the CMMC
- Guidance for preparing for a CMMC assessment, including a CMMC Compliance Checklist to guide your pre-assessment process
- How to find the right Registered Provider Organization (RPO) or CMMC Third-Party Assessment Organization (C3PAO) for your organization

WHAT IS CMMC?

CMMC is a unified approach to assessing the cybersecurity maturity of all companies seeking to contract with the US Department of Defense (DoD), where the data that is handled is classified as Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). The DoD introduced the CMMC framework in January 2020 to improve the cybersecurity of the US Defense Industrial Base – a vast supply chain comprised of more than 300,000 companies. Cybersecurity professionals know that any system is only as strong as its weakest link. Nation-states, sophisticated global criminal organizations, and even highly motivated individual actors actively seek out those weak links and pose an increasing cybersecurity threat. Given the breadth of the DIB, there is no shortage of potential targets for cybercriminals: each of the 300,000+ companies working for or with the DoD represents a potential breach.

In addition to the national security risks, there are economic impacts to cybercrime as well. The Council of Economic Advisers, an agency within the Executive Office of the President, estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016[1]. The Center for Strategic and International Studies (CSIS), in partnership with McAfee, reports that as much as $600 billion, nearly 1% of global GDP, may be lost to cybercrime each year. The estimate is up from a 2014 study that put global losses at about $445 billion[2].

Before the introduction of the CMMC, contractors were responsible for ensuring the cybersecurity of their information technology systems and any protected DoD information either stored or transmitted on those systems. While contractors remain ultimately responsible for adhering to cybersecurity requirements, the CMMC added an additional layer of diligence in assessing the organization's security posture by requiring third-party assessment and verification.

The U.S. government defines FCI as "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments" (from 48 CFR 52.204-21). Examples of FCI include emails transmitted between the DoD and its contractors and other information that may have been shared via conference calls or other methods of communication.

CUI is defined as "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls" (from 32 CFR 2002.4). Examples of CUI include intellectual property, technical drawings, blueprints, and other forms of related documentation, such as those for export control, cyber vulnerability information, and other sorts of financial data.

How do I know if I need to be CMMC certified?

The CMMC requirements apply to all DoD's DIB supply chain participants. In other words, if you wish to do business with the DoD or with contractors doing work for the DoD, you must attain a certain level of CMMC compliance. Prime contractors will be required to pass down some level of CMMC compliance to any of their in-scope sub-contractors.

Due to the large number of entities that make up the DIB, there is a staged rollout of CMMC across the industry. The current expectation is that it will take until 2026 for in-scope entities to complete the assessment process and obtain their certification.

Whether a DoD supplier or the sub-contractors of a prime are required to become certified is stated in the terms and conditions of the DoD contract. That contract will determine the maturity level the DoD requires the supplier to attain before the contract award.

Sub-contractors to a prime contractor are also required to meet a specific maturity level. The prime contractor will communicate the level that they are required to meet. It is the prime contractor's responsibility to ensure that all its sub-contractors meet the maturity level stated.

How does the CMMC certification process work?

As stated earlier, whereas previously, the DoD allowed contractors to self-assess and relied on an "honor" system for cybersecurity readiness, the CMMC requires certification by an independent, third-party entity. The Cyber Accreditation Body (Cyber AB) was established as an independent organization to authorize and accredit the CMMC Third Party Assessment Organizations (C3PAOs). C3PAOs are responsible for conducting the actual CMMC assessments of organizations aspiring to attain CMMC certification. The Cyber-AB also oversees the CMMC Assessors and Instructors Certification Organization (CAICO), ensuring that assessors are appropriately trained, tested, authorized, and certified to perform assessments per DoD requirements.

While self-certification is allowed for Level 1certification, companies can complete an initial self-assessment based on **CMMC Assessment Guides published by the DoD**. However, many companies opt to partner with organizations like Dewpoint to guide them through this process.

To undertake a formal certification assessment, companies must select an Authorized or Accredited C3PAO from the **Cyber-AB Marketplace**. The company and the C3PAO work together to conduct the CMMC assessment. Upon completion, the C3PAO delivers an assessment report to the Cyber-AB for review; if the Cyber-AB agrees that the assessment has been completed successfully, it will issue the appropriate certificate and submits a copy of the report and certificate to the DoD.

What is the next step in the CMMC certification process?

The next step in CMMC compliance is understanding the maturity levels defined by the CMMC and determining which level your organization needs to obtain.

As a Registered Provider Organization (RPO), Dewpoint Registered Practitioners (RPs) can provide design and implementation services to meet CMMC practices and assist in creating CMMC required documentation. In addition, Dewpoint RPs can help you prepare for your certification assessment by performing readiness assessments based on people, processes, and technology to evaluate your current security program utilizing a proven methodology and IT expertise to provide you with actionable recommendations to meet your desired CMMC maturity level.

UNDERSTANDING CMMC MATURITY LEVELS

The CMMC framework has three escalating maturity levels, from foundational to expert, related to the type of DoD or US government data that an organization may be interacting with. The maturity levels are graded and align to the depth and completeness with which an organization has implemented and operationalized its security program. The framework organizes best practices and maturity processes into domains mapped across the three maturity levels. The processes range from Level 1, "Foundational," to Level 3, "Expert." Within each domain, these best practices are aligned with corresponding capabilities. To obtain certification at a specific level, organizations must demonstrate the institutionalization and implementation of the practices. Due to the cumulative nature of the framework, organizations must meet the requirements of all levels preceding the level for which they are seeking certification.

Understanding which level of maturity your organization needs to attain and the capabilities required for each level is critical to your ability to work with the DoD on desired projects.

The DoD's stated goal is for the CMMC to be "cost-effective and affordable for small businesses to implement at the lower CMMC levels."

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

LEVEL 1:

Foundational Cyber Hygiene

The purpose of Level 1 is to safeguard FCI by ensuring that organizations meet a basic level of cyber hygiene. Organizations must perform the specified practices, but process maturity is not assessed at this level. It is understood that organizations may lack documentation and perform practices in an ad-hoc fashion. The 17 Practices related to the basic safeguarding of FCI span 6 Domains and are specified 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 builds on the foundation of Level 1 expectations and is a transitional step in the journey to protecting CUI. To obtain Level 2 certification, organizations must document their cyber hygiene processes and practice them as documented. The 110 practices related to Level 2 span 17 Domains and align with the NIST SP 800-171 documentation.

LEVEL 3:

Expert Cyber Hygiene

Level 3 builds on Levels 1 and 2, with the goal of protecting CUI. In order to attain Level 3 certification, organizations must demonstrate that their processes are properly managed. This requires the development and maintenance of a comprehensive plan with includes resourcing, training, project plans, and other details.

The 110+ Practices required in Level 3 span 17 domains, with 110 Practices from NIST SP 800-171 and a selection of practices from NIST SP 800-172.

HOW TO PREPARE FOR A CMMC ASSESSMENT:
PRE-ASSESSMENT CMMC COMPLIANCE CHECKLIST

Before you begin the CMMC assessment process, review this CMMC compliance checklist. If there are gaps in your data, documentation, or practices, now is the time to address them.

1. Determine the CMMC level that your organization needs to attain.
2. Determine the scope of the data that the assessment will cover.
3. Establish the boundaries as to how data is managed and handled to put boundaries around the assessment.
4. Review all processes and the level of documentation that exists for each of the processes.
5. Fill in any documentation gaps that may have been identified.
6. Review all relevant practices and determine who performs these practices. Determine if the identified individuals can speak to how they perform the tasks.
7. Determine if your organization can conduct these pre-assessment activities or will need help from an outside specialist.

CMMC Compliance Checklist

As you prepare for a CMMC assessment, reviewing your organization's capabilities across the 17 domains associated with the CMMC model is essential. The checklist below provides a high-level overview; within each domain and across all three levels.

CMMC DOMAIN	CAPABILITY (SAMPLE ONLY)
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
Maintenance (MA)	· Manage maintenance
Media Protection (MP)	· Identify and mark media · Protect and control media · Sanitize media · Protect media during transport
Personnel Security (PS)	· Screen personnel · Protect CUI during personnel actions
Physical Protection (PE)	· Limit physical access
Recovery (RE)	· Manage back-ups
Risk Management (RM)	· Identify and evaluate risk · Manage risk
Security Assessment (CA.)	· Develop and manage a system security plan · Define and manage controls · Perform code reviews
Situational Awareness (SA)	· Implement threat monitoring
System and Communications Protection (SC.)	· Define security requirements for systems and communications · Control communications at system boundaries
Systems and Information Integrity (SI)	· Identify and manage information system flaws · Identify malicious content · Perform network and system monitoring · Implement advanced email protections

The journey to preparing for a CMMC assessment will not be short. Organizations are advised to allow six months or more to prepare for and undergo an assessment.

Pre-Assessment Process

To prepare for a formal CMMC assessment, it is recommended that organizations that have not undergone formal NIST SP 800-171 assessments engage with an organization that has the skills and experience to help them prepare for such an activity. The Cyber AB created a **Marketplace** to help organizations identify businesses that have undertaken the prerequisite education and completed the necessary background validation required by the Cyber-AB to conduct pre-assessment engagements. Organizations that have undergone such activities are designated as Registered Provider Organizations (RPO), or they may be CMMC Third Party Assessment Organizations (C3PAO).

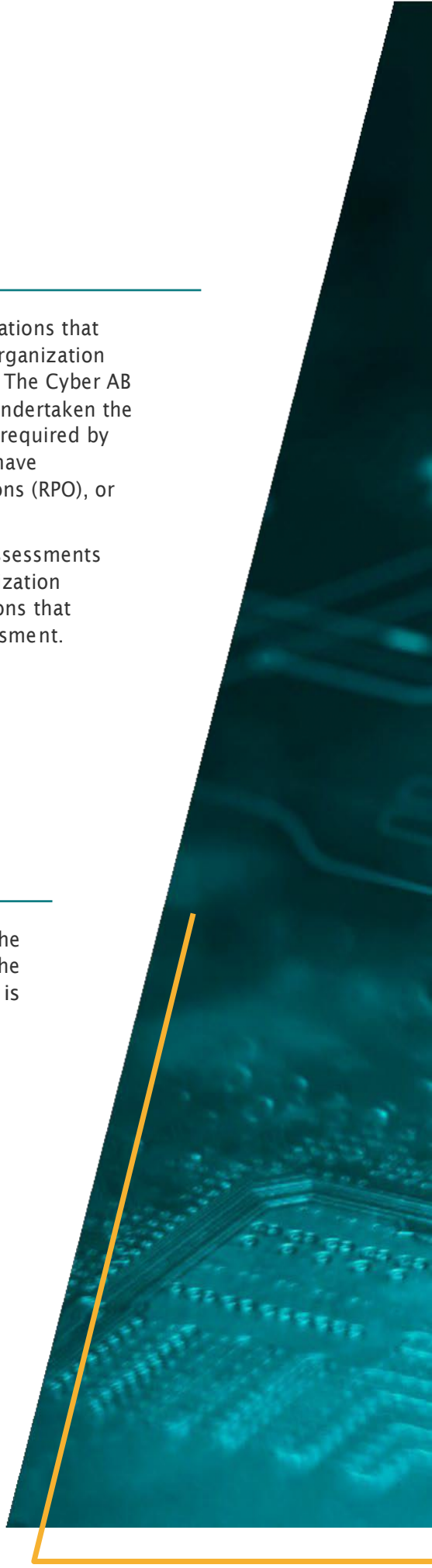
The CMMC program has been designed to ensure that the integrity of the assessments meets the highest standards. As such, the Cyber AB requires that the organization conducting the final assessment has no conflicts of interest with organizations that may have been engaged to assist in preparing a business for the final assessment.

The Formal Assessment Process

Once an organization is prepared for its final assessment, it engages with the selected C3PAO. The C3PAO will assign a Certified Assessor (CA) to lead the assessment. The assessment contract is between the organization that is being assessed and the C3PAO.

Certification

Upon completion of the assessment, the CA will submit their assessment report to their C3PAO internal review panel for an internal quality review. If the quality review is successful, the C3PAO will submit the assessment to the Cyber-AB for its quality assessment review. A successful review by the Cyber-AB will lead to the issuance of a certificate. CMMC certificates are valid for three years and are issued to a specific maturity level and for only those areas of the organization that was part of the assessment scope.



Finding the Right RPO

As a Registered Provider Organization (RPO), Dewpoint Registered Practitioners (RPs) can provide design and implementation services to meet CMMC practices and assist in creating CMMC required documentation. In addition, Dewpoint RPs can help you prepare for your certification assessment by performing readiness assessments based on people, processes, and technology to evaluate your current security program utilizing a proven methodology and IT expertise. The outcome of this assessment will provide you with actionable recommendations to meet your desired CMMC maturity level.

Dewpoint offers expert assistance and solutions to help you successfully prepare for your CMMC certification assessment.

READINESS ASSESSMENTS:

Review security program controls against the required CMMC level to identify gaps and provide remediation recommendations

DEVELOP 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:

Provide support creating and updating POA&M (for internal use only during gap remediation activities, limited PAO&M's are acceptable for a final CMMC assessment)

DEVELOP CMMC PROCESSES:

Assist in creating CMMC required processes such as policies, standards, and other supporting documentation

TECHNICAL IMPLEMENTATION SERVICES:

Assist in remediation activities by providing architecture and technical project implementation support

PROVIDE PROGRAM MANAGEMENT EXPERTISE:

Create and update the ongoing governance necessary to maintain CMMC compliance

ONGOING SUPPORT AND CISO-AS-A-SERVICE:

Provide ongoing support to ensure compliance since adherence to the CMMC is a continuous requirement and not a one-time task

Additional Resources

- Cyber AB Accreditation Body
- Office of the Under Secretary of Defense for Acquisition & Sustainment
- CMMC FAQs
- Townhalls
- Cybersecurity Maturity Model Certification

"Achieving CMMC compliance will ensure your company's ability to **maintain** and **increase DoD contracts** and **stay ahead of your competition."**

Don Cornish,
Chief Information Security Officer

DEWPOINT

For More Information, Contact Dewpoint
https://www.dewpoint.com/cmmc/

Sources:

1: "The Cost of Malicious Cyber Activity to the US Economy, CEA" February 2018

2: "Economic Impact of Cybercrime - No Slowing Down" February 2018