



CMMC GUIDE & COMPLIANCE CHECKLIST

2025 Edition



**PROTECT YOUR
BUSINESS FROM
CYBERCRIME**



INTRODUCTION

Navigating Cybersecurity Maturity Model Certification, or CMMC, can be a daunting task for companies of all sizes. In this 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 Certified 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.

Beyond national security risks, cybercrime carries massive economic impacts. USAID has said the costs of cybercrime could reach \$23 trillion by 2027. In the IBM Cost of a Data Breach Report, the United States ranked first among all countries and regions for the average cost of a data breach at \$9.36M.

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.

FCI Definition

FCI is defined 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" (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 Definition

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 governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls" (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 CMMC compliance to any of their in-scope sub-contractors.

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.

The prime contractors will communicate the level that sub-contractors 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?

CMMC certification requires an official assessment by an independent, third-party entity. The Cyber Accreditation Body (Cyber AB) was established to authorize and accredit CMMC Third-Party Assessment Organizations (C3PAOs).

Contractors to the DoD can work with Registered Practitioner Organizations (RPOs) to prepare for an official C3PAO assessment. [Learn more about Dewpoint's CMMC services.](#)

Self-assessment is permitted for Level 1 and, dependent on the sensitivity of the CUI data involved, for some Level 2 certifications. Each DoD procurement contract will specify the applicable CMMC requirement.

When an organization decides it is ready for certification, it must select an authorized C3PAO from the Cyber AB Marketplace. The organization being assessed and the C3PAO will work together to complete the official assessment. Upon completion, the C3PAO will deliver an assessment report to the Cyber AB for review. If the Cyber AB confirms that the assessment has been passed, it will issue the appropriate certificate and submit a copy of the assessment report to the DoD.



What is the next step in the CMMC certification process?

Determine which level of CMMC your organization needs to meet and understand the practices associated with that level.

As a Registered Practitioner Organization (RPO), Dewpoint can provide remediation services, including document creation, to meet CMMC practices. Our Registered Practitioners (RPs) evaluate people, processes, and technology using a proven methodology. With deep cybersecurity expertise, the Dewpoint RPs can provide organizations with actionable recommendations to meet the desired CMMC level.

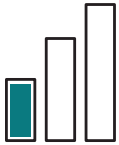


UNDERSTANDING CMMC MATURITY LEVELS

The CMMC framework has three escalating maturity levels 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.

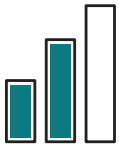
Understanding which level of maturity your organization needs to attain and the capabilities required for each level is critical to your ability to work with the DoD on desired projects.

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



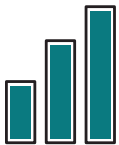
LEVEL 1:
Foundational Cyber Hygiene

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 15 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 and is a transitional step in the journey of 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 NIST SP 800-171.



LEVEL 3:
Expert Cyber Hygiene

Level 3 builds on Level 2, requiring robust protection of CUI. In order to attain Level 3 certification, organizations must demonstrate that their processes are properly managed. Organizations must develop and maintain a comprehensive plan including resourcing, training, project plans, and other details.

The 124 Practices required for Level 3 span 17 domains, with 110 Practices from NIST SP 800-171 and 24 practices from NIST SP 800-172.



HOW TO PREPARE FOR A CMMC ASSESSMENT: COMPLIANCE CHECKLIST

Organizations are advised to allow at least six months to prepare for and undertake an official CMMC assessment. For levels 2 and 3, multiple months of documentation showing that processes have been appropriately followed will be required.

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.

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 how data is accessed and managed to limit the scope of the assessment.

4 Review all processes and the documentation that exists for each one.

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 of each domain.

CMMC DOMAIN	CAPABILITY (SAMPLE ONLY)
Access Control (AC)	<ul style="list-style-type: none"> • Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	<ul style="list-style-type: none"> • Identify and document assets
Audit and Accountability (AU)	<ul style="list-style-type: none"> • Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	<ul style="list-style-type: none"> • Conduct security awareness activities • Conduct training
Configuration Management (CM)	<ul style="list-style-type: none"> • Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	<ul style="list-style-type: none"> • Grant access to authenticated entities
Incident Response (IR)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Manage maintenance
Media Protection (MP)	<ul style="list-style-type: none"> • Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	<ul style="list-style-type: none"> • Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	<ul style="list-style-type: none"> • Limit physical access
Recovery (RE)	<ul style="list-style-type: none"> • Manage back-ups
Risk Management (RM)	<ul style="list-style-type: none"> • Identify and evaluate risk • Manage risk
Security Assessment (CA)	<ul style="list-style-type: none"> • Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	<ul style="list-style-type: none"> • Implement threat monitoring
System and Communications Protection (SC)	<ul style="list-style-type: none"> • Define security requirements for systems and communications • Control communications at system boundaries
Systems and Information Integrity (SI)	<ul style="list-style-type: none"> • Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections



Pre-Assessment Process

It is recommended that organizations that have not undergone a formal NIST SP 800-171 assessment engage with a provider with the skills and experience to help them prepare for a formal CMMC assessment. The Cyber AB created a [marketplace](#) to help businesses locate Registered Practitioner Organizations (RPOs)—including Dewpoint—and CMMC Third-Party Assessment Organizations (C3PAOs). RPOs are specially trained to help companies prepare for formal C3PAO assessments.

The CMMC Program has been designed to ensure the integrity of the assessments meets the highest standards. The Cyber AB requires that the C3PAO conducting the final assessment has no conflicts of interest with organizations that may have been engaged to prepare the business.



The Formal Assessment Process

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



Certification

Upon completion, the CA will submit their assessment report to their C3PAO internal review panel for a 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 were part of the assessment scope.

Annual Attestation: Organization leaders must complete an annual attestation, affirming that the organization is maintaining the same standards and processes as when it was assessed by a C3PAO.

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 SSP's

PLAN OF ACTION AND MILESTONES (POA&M) DEVELOPMENT:

Provide support creating and updating POA&M (for internal use only during gap remediation activities, PAOM's are not 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

“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](#)
3. [IBM Cost of a Data Breach Report 2024 | January 2024](#)

Additional Resources

1. [CMMC FAQ | U.S. Department of Defense](#)
2. [Cyber AB | Townhall Video Recordings](#)
3. [Dewpoint | About CMMC](#)