CMMC

Cybersecurity Maturity Model Certification

(V 2.0) - NIST SP 800-171 AND NIST SP 800-172

AN EXECUTIVE OVERVIEW

Revised 3/2022

PERRY JOHNSON CONSULTING, INC.

Detroit

200 East Big Beaver Rd. • Troy, Michigan 48083
1-888-248-0256 or (248) 519-2602

Website: www.pjcinc.com • **Email:** pjc@pjcinc.com

CMMC

Cybersecurity Maturity Model Certification

(V 2.0) - NIST SP 800-171 AND NIST SP 800-172

An Executive Overview

CONTENTS

FOREWORD

The purpose of the document is to provide an executive overview of CMMC (Cybersecurity Maturity Model Certification) requirements.

This guide was written to provide information about the CMMC framework model, and its applications. It outlines the general requirements of CMMC, which can be applied to any type of industry or company that has electronic information that must be kept secure.

Certification to CMMC offers a major competitive edge for organizations that handle electronic data and it is a mandatory requirement for Defense Industrial Base (DIB) sector. Unlike ISO 27001 or SOC 2 certification, CMMC is a mandatory requirement for both prime and subcontractors to the DoD. Starting in 2020, companies that lack a current CMMC certification will be unable to bid on or participate in a DoD contract. This makes CMMC a "must have" business requirement versus a "nice to have" certification for marketing purposes. In addition to the loss of potential business, non-compliance with NIST 800-171 and CMMC can lead to serious legal consequences to both individuals and the company through False Claims Act (FCA) violations.

Of course, not every company that handles sensitive electronic data is the same. The CMMC offers flexibility in approach and levels, but its requirements must be implemented in full. To determine how to approach these various requirements, interested organizations should hire the services of a reputable CMMC consulting firm.

Firms planning a certification to adopt CMMC should obtain the aid of a reputable consulting company in implementing the existing requirements of the framework.

PERRY JOHNSON CONSULTING, INC.
March 2022

FAQ

What is the need for CMMC?

The aggregate loss of controlled unclassified information (CUI) from the DIB (Defense Industrial Base) sector increases risk to national economic security and in turn, national security. In order to reduce the risk, the DIB sector must enhance its protection of CUI in its networks.

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 [Ref: "The Cost of Malicious Cyber Activity to the U.S. Economy, CEA" in Feb 2018].

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. [Ref: "Economic Impact of Cybercrime - No Slowing Down" in Feb 2018].

DOD (Department of Defense) is planning to migrate to the new CMMC framework in order to assess and enhance the cyber security posture of the DIB. The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cyber security practices and processes are in place to ensure basic cyber hygiene as well as to protect CUI that resides on the Department's industry partners' networks.

What is CMMC?

CMMC stands for "Cybersecurity Maturity Model Certification". The CMMC will encompass multiple maturity levels that range from "Basic Cyber Security Hygiene" to "Advanced/ Progressive". The intent is to incorporate CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a requirement for contract award.

What is the version of CMMC as of March 2022?

Version 2.0, 03 Dec 2021

What are the relationships between similar frameworks and CMMC?

CMMC Levels 1-2 encompass the 110 security requirements specified in NIST SP 800-171. CMMC incorporates additional practices and processes from other standards such as NIST SP 800-172.

How will my organization be certified?

The CMMC Accreditation Body (AB), a non-profit, independent organization, will accredit CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors. The CMMC AB will provide the requisite information and updates on its website (www.cmmcab.org).

The CMMC AB established a CMMC Marketplace that includes list of approved C3PAOs as well as other information. DIB companies can select one of the approved C3PAOs and schedule a CMMC assessment for a specific level.

Will there be a Self-Certification?

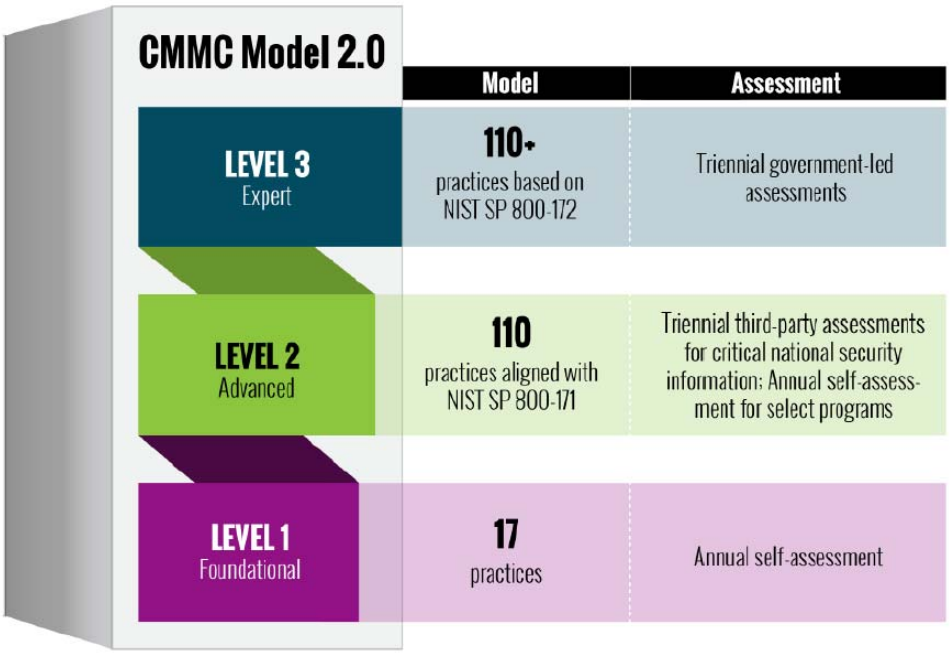
Yes, Self-Certification is allowed for Level 1 only to those companies that are only required to protect the information systems on which FCI is processed, stored, or transmitted.

For Level 2, Self-Certification is allowed for subset of companies (non-critical) that are required to protect CUI.

THE TIMELINE OF CMMC

- May 2019: CMMC version 0.1 released
- July 2019: CMMC versions 0.2 identified and reviewed
- September 2019: CMMC version 0.4 released
- October 2019: CMMC implemented requirements released
- November 2019: CMMC version 0.6 to be released for public review
- January 2020: CMMC Version 1.0 Released
- March 2020: CMMC Version 1.02 Released
- September 2020: CMMC Will Begin Appearing in RFPs
- Dec 2021: CMMC V2.0 Released

CMMC FRAMEWORK STRUCTURE



CMMC DOMAINS

The CMMC model consists of 14 domains that align with the families specified in NIST SP 800-171. These domains and their abbreviations are as follows:

- Access Control (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (CA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

CMMC DOMAINS AND CAPABILITIES

17 domains consists of 43 capabilities

Domain	Capability
Access Control (AC)	• Establish system access requirements
	• Control internal system access
	• Control remote system access
	• Limit data access to authorized users and processes
Awareness and Training (AT)	• Conduct security awareness activities
	• Conduct training
Audit and Accountability (AU)	• Define audit requirements
	• Perform auditing
	• Identify and protect audit information
	• Review and manage audit logs
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
Risk Management (RM)	• Identify and evaluate risk
	• Manage risk
	• Manage supply chain risk
Security Assessment (CA)	• Develop and manage a system security plan
	• Define and manage controls
	• Perform code reviews
Systems and Communications Protection (SC)	• Define security requirements for systems and communications
	• Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws
	• Identify malicious content
	• Perform network and system monitoring
	• Implement advanced email protections

CMMC LEVELS

CMMC Levels	Maturity Process Levels Title	Description
Level 1	Foundational	Focuses on the protection of FCI and consists of only practices that correspond to the basic safeguarding requirements – 17 practices
Level 2	Advanced	Focuses on the protection of CUI and encompasses the 110 security requirements specified in NIST SP 800-171
Level 3	Expert	Subset of NIST SP 800 – 172 requirements

CMMC CONTROL MATRIX

Domains	NIST 800-171 Controls	NIST 800-172 Enhanced Controls
Access Control	22	3
Awareness and Training	3	2
Audit and Accountability	9	0
Configuration Management	9	3
Identification and Authentication	11	3
Incident Response	3	2
Maintenance	6	0
Media Protection	9	0
Personnel Security	2	2
Physical Protection	6	0
Risk Assessment	3	7
Security Assessment	4	1
System and Communications Protection	16	5
System and Information Integrity	7	7
Total - 14	**110**	**35**

CMMC DOMAIN vs ISO/IEC 27002:2013 MATRIX

Domain	Capability	ISO/IEC 27002:2013
Access Control (AC)	• Establish system access requirements	A.9.1
	• Control internal system access	A.9.1
	• Control remote system access	A.6.2
	• Limit data access to authorized users and processes	-
Awareness and Training (AT)	• Conduct security awareness activities	A.7.2.2
	• Conduct training	A.7.2.2
Audit and Accountability (AU)	• Define audit requirements	A.12.7.1
	• Perform auditing	A.12.7.1
	• Identify and protect audit information	A.12.7.1
	• Review and manage audit logs	-
Configuration Management (CM)	• Establish configuration baselines	A.8
	• Perform configuration and change management	A.12.1.2
Identification and Authentication (IA)	• Grant access to authenticated entities	A.9.3.1
Incident Response (IR)	• Plan incident response	A.16.1.1
	• Detect and report events	A.16.1.2
	• Develop and implement a response to a declared incident	A.16.1.5
	• Perform post incident reviews	A.16.1.6
	• Test incident response	A.17.1.3
Maintenance (MA)	• Manage maintenance	A.12.1
Media Protection (MP)	• Identify and mark media	A.8.3
	• Protect and control media	A.8.3
	• Sanitize media	-
	• Protect media during transport	A.8.3.3
Personnel Security (PS)	• Screen personnel	A.7.1.1
	• Protect CUI during personnel actions	A.7.2, A.7.3
Physical Protection (PE)	• Limit physical access	A.11.1
Recovery (RE)	• Manage backups	A.12.3
	• Manage information security continuity	A.17.1
Risk Management (RM)	• Identify and evaluate risk	ISO/IEC 27001:2013, 6.1
	• Manage risk	
	• Manage supply chain risk	A.15.1/A.15.2
Security Assessment (CA)	• Develop and manage a system security plan	A.14.1
	• Define and manage controls	A.14.1
	• Perform code reviews	A.14.2.1
Systems and Communications Protection (SC)	• Define security requirements for systems and communications	A.10/A.11/A.12/A.14
	• Control communications at system boundaries	
System and Information Integrity (SI)	• Identify and manage information system flaws	A.14.2.3
	• Identify malicious content	
	• Perform network and system monitoring	A.13.1
	• Implement advanced email protections	A.13.2

CERTIFICATION TO CMMC

Following are the recommended steps towards achievement of Certification to CMMC:

1. Select a reputed consultancy partner to guide the certification project
2. Perform gap assessment against the intended security level
3. Awareness training of CMMC
4. IT asset inventory and classification of assets and define the scope
5. Selection of third-party assessment organizations approved by CMMC AB
6. Prepare documentation (Policies, Processes, Procedures, WI, Plans, etc.)
7. Perform risk assessment/evaluation/risk treatment
8. Selection of practices for identified risks
9. Prepare system security plan
10. Implementation of all processes/practices to the intended level of certification
11. Implement monitoring and measurements
12. Analysis and evaluation of measurements
13. Train internal auditors
14. Perform internal audits and capture levels of processes and practices
15. Report levels to top management and review for changes
16. Readiness Audit by the C3PAO
17. Corrective action
18. Certification audit by the selected third-party assessment organization
19. Corrective action for the identified deficiencies, if any
20. Certification

Remember: In order to achieve registration to CMMC, the organization must completely embrace the framework; Top management must demonstrate commitment in defining the policies, plans, providing resources timely and periodically review the implementation progress, level of compliance to ISMS and its effectiveness.

THE BENEFITS OF CMMC CERTIFICATION

Key benefit is the opportunity to respond to RFP/RFQ from DoD based on the level described in the RFP/RFQ.

The benefits of implementing ISMS (Information Security Management System) are realized most significantly in the reduction of information security risks. This means not that such incidents will never happen, but rather that their likelihood is reduced and impact is lessened.

CONCLUSION

An organization that chooses to conform to CMMC will be operating a top-notch information security management system that focuses on informed and competent management decision making, control of risks, and reduced waste.

REFERENCES

1. ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements
2. ISO/IEC 27002:2013; Information technology — Security techniques — Code of practice for information security controls
3. Cybersecurity Maturity Model – Version 2.0, Dec 03, 2021
4. CMMC Model – FAQs and Other Documents: https://www.acq.osd.mil/cmmc/index.html