FORNETIX

CMMC 2.0 Gap Assessment

The Cybersecurity Maturity Model Certification (CMMC) program enhances cyber protection standards for government contractors. It is designed to protect sensitive unclassified information that is shared by the government with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides increased assurance that contractors are meeting these requirements. CMMC 2.0 is the next iteration of the Department of Defense's CMMC cybersecurity model. It streamlines requirements to three levels of cybersecurity – Foundational, Advanced, and Expert – and aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards. The Department of Defense (DoD) expects defense contractors to achieve CMMC certification as the program rolls out.

Purpose

The purpose of CMMC is to ensure that the DoD's critical supply chain is protected from cybersecurity threats. The verification mechanism protects Federal Contract Information (FCI), Controlled Unclassified Information (CUI), and Covered Defense Information (CDI), which is CUI specifically related to defense products and services. What is critical to consider is that the evaluation of controls for Cybersecurity has application outside of Federal services. Even if CMMC is not a business objective, a Cybersecurity Gap Assessment tailored for CMMC will identify Cybersecurity strengths and weaknesses in your organization.

How Fornetix Can Help — Cybersecurity Gap Assessment

Fornetix will perform a system architecture review, policy audit, operational, managerial, and technical controls review, and IT business process assessment to determine the current state of the security architecture of the system as it relates to CMMC compliance. An interview, examination, and verification will be performed to measure the current state of conformance to the specific CMMC Level you desire to achieve. Fornetix will provide a final Cybersecurity Assessment Report, documenting the current security posture of the organization based on the CMMC Level of compliance you are working towards. This will be used as a road map, which will identify security gaps/weaknesses to be resolved prior to scheduling your official CMMC certification audit.

Our Approach

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6	STEP 7	STEP 8	STEP 9
Collect the information we need to assess risks. Find all valuable assets across the organization.	Identify potential threats.	Identify vulnerabilities.	Analyze controls.	Assess the likelihood of vulnerability exploitation.	Assess impact a threat could have.	Determine risk level.	Recommend controls.	Document the results and define mitigation processes.

Fornetix will utilize the Cybersecurity Assessment Report to identify key remediation steps that will reduce multiple risks. For example, ensuring backups are taken regularly and stored offsite will mitigate the risk of accidental file deletion and facilitates recovery from a ransomware attack. Each of these steps have the associated cost and deliver real benefit in reducing the risks. We focus on the business reasons for each implementation.

CMMC 2.0 Timeline

Effective November 30, 2020, defense contractors must self-assess their implementation of all 110 NIST 800-171 controls and enter their score on a federal website to qualify for future contracts. An estimated 300,000+ defense contractors will need to become CMMC certified. DoD intends to implement CMMC 2.0 through a notice-and-comment rulemaking process which can take anywhere from 9 to 24 months, as opposed to the previously planned rollout by FY 2026, which now significantly reduces the CMMC implementation timeline.

CMMC 2.0 Assessments

Every entity that seeks CMMC certification will be audited. The CMMC assessments performed will be an annual self-assessment and Supplier Performance Risk System (SPRS) affirmation or triennial assessment by either an independent or government assessor depending on certification level.

Non-Compliance

If a business fails to achieve CMMC certification, it will not be permitted to bid on defense contracts. Failure to maintain compliance with the certification standards may result in the loss of government contracts, breach of contract lawsuits, potential violations of the federal False Claims Act, and banishment from future contracts.

CMMC 2.0 Levels

	Model	Assessment
Level 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
Level 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
Level 1 Foundational	**17** practices	Annual self-assessment

How Fornetix VaultCore Helps With CMMC 2.0 and NIST SP 800-171

The VaultCore platform supports implementation of the following controls for the protecting CUI:

3.1.12	Monitor and control remote access sessions.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
3.1.17	Protect wireless access using authentication and encryption.
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
3.8.9	Protect the confidentiality of backup CUI at storage locations.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
3.13.16	Protect the confidentiality of CUI at rest.