Carnegie Mellon University
Software Engineering Institute

CMMC

Securing the DIB Supply Chain with the Cybersecurity Maturity Model Certification Process

What is Process Maturity?

Process maturity represents an organization's ability to institutionalize, or embed, its processes. Measuring process maturity indicates how well a company has ingrained practices and processes in the way it defines, executes, and manages work. In addition, process maturity represents an organization's commitment and consistency to performing these processes.

A high degree of process maturity, or process institutionalization, contributes to more stable processes. This stability produces consistent and expected results over time. Organizations are able to retain mature processes during times of stress. Specifically, in the case of cybersecurity, having mature cybersecurity processes and practices will improve an organization's ability to both prevent and respond to a cyberattack.

Process Maturity in CMMC

The Process Maturity dimension in the Cybersecurity Maturity Model Certification (CMMC) represents a fundamental shift from a compliance, checklist-based perspective to an approach that is focused on continuous improvement and, ultimately, changing an organization's culture.

A company is assessed for process maturity for CMMC practices at Maturity Levels (ML) 2-5 for each of the 17 CMMC domains. At ML 1, Process Maturity is not formally assessed. An organization is expected to be performing practices at ML 1.

SEI Expertise

The SEI has a long and accomplished history with process maturity and measurement. CMMC is a product of this experience, specifically, of two long-validated SEI cybersecurity models: CMMI and CERT-RMM.

The SEI developed Capability Maturity Model Integration (CMMI) more than 25 years ago to help organizations achieve repeatable and sustainable results. This seminal work measures the performance of a range of critical business capabilities.

We combined our CMMI work with the SEI's deep expertise in resilience and cybersecurity to develop the CERT Resilience Management Model, or CERT-RMM. CERT-RMM defines the practices and metrics needed to manage operational resilience.

The CERT-RMM is the basis for planning, communicating, and evaluating improvements across an enterprise. It is foundational in the design and development of the CMMC architecture and process maturity.

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

Example: Access Control

The following example examines how AC.1.001 progresses through CMMC process maturity levels.

AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ML1 PERFORMED

The organization performs the CMMC practices as defined. (Process Maturity is not formally assessed.)

Bob is in charge of IT. He assigns everyone a username and password if they are allowed to be on the system. He ensures that everyone can access only what they have permission to access. Bob is performing AC.1.001. At ML 1, CMMC does not formally assess process maturity.

ML2 DOCUMENTED

The organization has documented all Access Control (AC) practices, and has an AC Policy.

Senior management recognizes the importance of Access Control, and develops a policy that includes the scope of the Access Control domain. This can be a specific Access Control policy or one or more policies that includes the scope of the CMMC Access Control domain. Bob makes sure he is following the defined Policy. This helps Bob understand the expectations for Access Control at his company, so that he can convey them properly to stakeholders. Bob documents all his Level 1 and Level 2 practices, including AC.1.001. This documentation articulates what needs to be done, so it can be repeated.

ML3 MANAGED

The organization has an Access Control Plan that is resourced accordingly.

Bob manages his Access Control activities according to a defined plan. The plan defines a mission statement, goals and objectives, required resources and tools, and identified training to achieve the Access Control objectives. This plan can be specific to just Access Control, or be an overarching plan, such as a IT security plan, that includes the scope of the CMMC Access Control domain. Bob makes sure resources are assigned as defined in the plan, which covers all practices for Access Control (including AC.1.001).

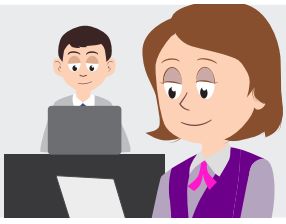
ML4 REVIEWED

The organization reviews and measures Access Control activities for effectiveness.

Bob establishes periodic reviews of Access Control activities, which include performance of AC.1.001. For example, he reviews access lists to make sure he disables accounts when responsibilities change or people leave the company. Bob defines and conducts periodic communications with high-level managers to review status, and to inform them of any issues.

ML5 OPTIMIZING

The organization has a standard approach for Access Control, and shares improvements throughout the enterprise.



Bob and Sue both do Access Control in different business units within the organization. They develop their procedures, including those for practice AC.1.001, from standard guidance that senior management typically provides. They also communicate and share improvement information they collect when carrying out the Access Control practices, to inform updates to standard guidance.