Carnegie Mellon University
Software Engineering Institute

CMMC Scoring

Understanding the Assessment Levels of the Cybersecurity Maturity Model Certification Process

In mid-2020, the Department of Defense (DoD) will require all Defense Industrial Base (DIB) organizations to achieve a level of Cybersecurity Maturity Model Certification (CMMC) before being permitted to bid on DoD contracts. DoD Program Managers will set the CMMC level—from 1 to 5—for each contract, and specify that level in the corresponding Request for Proposals (RFPs). However, each DIB organization decides on the CMMC level it wants to achieve, typically based on the DoD contracts it wants to bid on.

CMMC assessment is a cumulative activity. DIB organizations must demonstrate achievement for all practices and processes implemented at the CMMC level they are trying to achieve, as well as for all those at the preceding levels. For example, if a DIB company wants to be assessed at CMMC level 4, it must achieve all the practices and processes for levels 1 through 4. The following diagrams demonstrate the key components of CMMC scoring.

An organization is assessed for practices and processes.

The CMMC assesses organizations for a set of practices and associated processes based on the CMMC level the organization is trying to achieve. Note that process maturity is not assessed at Level 1, because an organization is expected to perform the CMMC practices at Level 1.

CMMC has five levels of practices and five levels of processes.

CMMC scoring is cumulative.

To receive a Level 3 certification, an organization must demonstrate Level 1, 2, and 3 practices as well as Level 2 and 3 processes. There are no Level 1 processes.

Achievement of Level 1, 2, and 3 practices, and Level 2 and 3 processes, results in a Level 3 certification.

An organization will receive only one CMMC level.

A CMMC level corresponds to the lower of the two scores, either practices or processes. For example, if an organization achieves levels 1, 2, and 3 practices but only Level 2 processes, it will receive a Level 2 certification.

Achievement of Level 1, 2, and 3 practices, but only Level 2 processes, results in a Level 2 certification.

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