THE CMMC ASSESSMENT LIFECYCLE

CMMC Information Institute

SELECT CMMC MATURITY LEVEL

IDENTIFY DATA IN YOUR ENVIRONMENT

The CMMC Maturity Level at which your organization, or an enclave within your organization, must be certified will depend on the nature of the information you create, process, store, or secure ("handle"). If you handle Controlled Unclassified Information (CUI), you must be certified at a minimum of Maturity Level 3. If you do not handle CUI, you must be certified at Maturity Level 1. If you are a COTS vendor, no CMMC certification is required.

GAP ANALYSIS

COMPARE CURRENT STATE AGAINST THE CMMC MODEL REQUIREMENTS

Review your organization's cybersecurity program against the practice and process requirements, and corresponding objectives, described in the CMMC Model and CMMC Assessment Guide. Collect Objective Evidence (e.g., screen captures, audit logs, interviews with stakeholders, etc.) that demonstrates how the organization meets each objective for, or how the objective is not applicable to, each system that is involved in the creation, receipt, storage, processing, or transmission of the government's information (i.e., the "in scope" systems. Any applicable objectives that are not met are "gaps".

GAP REMEDIATION

CLOSE ANY GAPS

To obtain a certification at a particular CMMC Maturity Level, your organization must demonstrate that its cybersecurity program has successfully adopted all of the practice and process requirements defined for that Maturity Level. No open items (gaps) are permitted.

ASSESSMENT PREPARATION

COLLECT OBJECTIVE EVIDENCE

After the gaps are closed, review Objective Evidence collected during the previous stages to ensure you have evidence for each practice and process, and the applicable corresponding objectives defined in the CMMC Assessment Guide. At least two forms of Objective Evidence (one from each category of "Examine", "Interview", and "Test") will be needed for the assessment. Careful execution of this step ensures a smoother pre-assessment readiness review and assessment.

PRE-ASSESSMENT READINESS REVIEW

ENSURE EVIDENCE IS READY FOR ASSESSMENT

The Lead CMMC Certified Assessor ("CA") assigned by the C3PAO will review your Objective Evidence for completeness but not for content. If gaps are found, the CA will identify those for you, but cannot provide advice on how to close those gaps.

ASSESSMENT

REVIEW OF OBJECTIVE EVIDENCE BY ASSESSMENT TEAM

The Assessment Team assigned by the C3PAO will review the content of the Objective Evidence you selected to ensure it demonstrates sufficient adoption of the applicable practices and processes for the CMMC Maturity Level at which you are being assessed and seeking certification.

MAINTENANCE

EMBED CYBERSECURITY INTO ORGANIZATIONAL CULTURE

After your organization's cybersecurity program is certified, you must continue to follow all of the applicable CMMC practices and processes. Certifications are valid for 3 years.

Steps you or your consultant can do are in green. Steps a C3PAO and/or Certified Assessor must do are in red.

CMMC INFORMATION INSTITUTE
CMMCInfo.org