5 Steps to CMMC Readiness

1. START PREPARING TODAY

Acting now is key to success. There is no standard timeframe for how long the CMMC process takes. It may take smaller companies less time than a larger or more sophisticated organization. And depending upon what level criteria you must meet, putting together the required documentation, such as a gap analysis and POAM (see more on this in step 5), can take six to nine months alone. If you fail the audit, you may be able to correct any deficiencies found in the assessment

2. CONDUCT A SELF-ASSESSMENT

To help streamline the CMMC process, the DoD requests that you complete a self-assessment before scheduling your CMMC assessment. Conducting self-audits or self-assessments in advance will also help you cut down on CMMC certification costs.

3. CONSULT WITH A CMMC PROFESSIONAL OR C3PAO

While the DoD has a website that vendors can use for guidance, contact information and to submit their assessments, consulting with a firm that provides CMMC assessment or a certified third-party assessor (C3PAO) is also a good idea. The agency or assessor you contact can tell you precisely what your assessment will entail, and advise you on how to prepare.

4. PREPARE FOR YOUR CMMC AUDIT

Only a CP3AO is qualified to perform a CMMC audit. The extent of your audit will depend on the maturity level for which your organization wishes to be certified. The assessor will first speak with you to determine your needs and will request any documents required to evaluate your controls for protecting FCI or CUI. They will also inquire about the systems you're using and what services you are providing and supplying to the DoD. These documents may include diagrams of your environment, risk assessments, data from vulnerability scans and a list of in-scope controls.

5. SUBMIT YOUR CMMC ASSESSMENT

There's a scoring process in place that the DOD looks at when you submit your CMMC assessment. It scores based on the following three things:

1. Your self-assessment
2. Your System Security Plan (SSP): A detailed document including all 130 CMMC required controls, as well as relevant attachments. This must be submitted in the DoD's template.
3. Your Plan of Action and Milestones (POAM): This document outlines where you have gaps in your environment, processes, infrastructure, policies and procedures. This must be submitted in the DoD's template.

Demonstrating compliance with CMMC requires ongoing monitoring and evidence, which may be required weekly, monthly or quarterly, depending on the level of CMMC certification.