Q&A

Cybersecurity Maturity Model Certification

What is CMMC?

CMMC stands for Cybersecurity Maturity Model Certification and is a requirement for all suppliers in the national Defense Industrial Base (DIB) to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

How will my organization know what CMMC level is required for a contract?

Once CMMC 2.0 is implemented, DoD will specify the necessary CMMC level in the solicitation and in any Requests for Information (RFIs).

What's the difference between NIST 800-171 and CMMC?

Under CMMC 2.0, the "Advanced" level (Level 2) will be equivalent to NIST SP 800-171 while the "Expert" level (Level 3) will be based on a subset of NIST SP 800-172 requirements.

Will my organization need to be fully compliant in 9-24 months?

The publication of materials relating to CMMC 2.0 reflect the Department's strategic intent with respect to the CMMC program; however, CMMC 2.0 will not be a contractual requirement until the Department completes rulemaking to implement the program. The rulemaking process and timelines can take 9-24 months. CMMC 2.0 will become a contract requirement once rulemaking is completed.

If I think my organization has a score of 110, is it still prudent to have BV to assess my score to ensure that the tools and documentation meet DoD standards?

BV certified professionals performing the review/assessment will validate that you are indeed receiving an unbiased account of your true compliance level. BV has seen in the DIB that organizations believe that they are using compliant tools only to find out after evaluation that they invested in tools that are in fact not compliant. They then need to rip and replace which causes loss of time, investment, and increases compliance frustration overall. It is prudent to be fully compliant as soon as possible to meet contractual compliance before DoD requires it.

What are risks for self-certification?

Since internal IT departments may not be certified professionals in CMMC, this could lead to a situation where your organization inadvertently submits a faulty lower score to SPRS. As a result, your organization may have a False Claim Act issue with the DoD and may need to explain to a prime why your score has been reported incorrectly or must rip and replace technical controls because of faulty advice from non-certified professionals.

Why should I choose BVMC to help me become CMMC compliant?

Even as a Registered Provider Organization (RPO), BV has the same expert level assessors on staff as a C3PAO. BV has a registered practitioner and a provisional assessor, which is a market differentiator compared to your in-house IT team or other 3rd party consultants that have not been trained and certified by the CMMC-AB (Accreditation Board).

How much will a readiness assessment cost?

Costs depend on the results of the gap analysis. The analysis will determine if there are missing tools that need to be purchased as well as the required time needed to execute the necessary administrative controls that will have to be put in place. Typically, the cost of executing BV CMMC services is less than a non-certified 3rd party consultant or your internal IT team who may or may not be adequately certified to administer the pre-assessment. Using a non-certified expert could also lead to additional changes, driving up costs later in the process.

Additional Reference Resources

- Cybersecurity Maturity Model Certification (CMMC) (osd.mil)
- Download our CMMC FAQ's
- Black & Veatch Management Consulting is an approved Registered Provider Organization (RPO) with the ability to service organizations of any size.

BLACK & VEATCH
MANAGEMENT CONSULTING