Control Risks

Cybersecurity Maturity Model Certification (CMMC)

Helping you meet new guidelines set out by the US Department of Defense

To help protect its supply chain, the US Department of Defense (DoD) announced a new cyber security standard that must be met by every organization it does business with. This new standard, the Cybersecurity Maturity Model Certification, builds off existing guidance including the NIST 800-171 and aligns certification requirements to the level of sensitivity of the goods or services provided. The final version of this certification is expected in late January 2020—with compliance required in requests for proposals (RFPs) starting in October 2020. Here's what your organization should know to be prepared to meet these new standards:

Certifying your organization

Every private-sector organization doing business with the DoD, not just those handling sensitive information, will need to be certified by a third-party auditor at a level appropriate to its work for the DoD. This differs drastically from current standards:

	NIST 800-171	CMMC
Certification	Self	Third party
Who must comply	Organizations handling Controlled Unclassified Information (CUI)	**Anyone** doing business with the DoD
Number of controls	110	To be stipulated within contracts: ▸ Level 1 (basic): 17 ▸ Level 2 (intermediate): 72 ▸ Level 3 (good): 131 ▸ Level 4 (proactive): 157 ▸ Level 5 (advanced): 173
Compliance levels per control	Yes/no	1 (basic) to 5 (advanced)

- Existing contracts will have the requirement added when renewed or otherwise modified.
- Failure to gain certification by October 2020 means an inability to bid on new DoD work.
- Organizations will need to be certified by a "third-party auditor organization" (3PAO). This process is expected to be published in January 2020. Control Risks plans to become a 3PAO.

What can your organization do to prepare?

We recommend starting preparations now in order to be ready when the CMMC goes live. Pre-assessment work will allow organizations to plan and budget for compliance efforts in the new fiscal year.

Here are steps you can take:

- Assess your current cyber security controls and processes against the draft CMMC standard to understand where investment is required.
  - The certification process is expected to be like any other audit. Begin assessing your organizations current status against the draft standard **now.**
  - Evaluate your existing DoD contracts to identify the target level of compliance for your business.
- Leverage available resources now and budget for additional investments in the new fiscal year.
- Begin vetting organizations who have expressed the intent to become a 3PAO.
  - Control Risks intends to become a 3PAO once the process is published in January.
- Aim to be certified at the appropriate level by October 2020.

Control Risks can help

Whether you require level 1 or level 5 certification, Control Risks can help. We are a specialist risk consultancy that helps create secure, compliant and resilient organizations. We work with organizations on cyber threat, risk and maturity assessments, evaluating current preparedness and improving security in an intelligent, cost-effective and comprehensive way across the organization. This is done through a process of threat assessment, asset evaluation and gap analysis. Control Risks is experienced with auditing to current standards such as NIST 800-53, 800-171, CSF and ISO 27001, and we intend to become a verified third-party auditor organization with the DoD. Control Risks is well-positioned to assist you in the process of achieving the appropriate level of CMM certification.

Connect with our expert

Mike Waters
Director, Cyber Security
Washington DC
Mike.Waters@controlrisks.com
+1 202-449-3331

- Specializes in helping companies incorporate cyber security into business strategies
- Over 20 years of cyber expertise, previously with a large defense contractor

www.controlrisks.com