General

The Cyber Maturity Model Certification

Securing the DoD supply chain

By October 2020, private sector companies must achieve Cyber Maturity Model Certification (CMMC) to compete for DoD business. Are you ready?

What do I need to know?

The CMMC is designed to protect organizations in the DoD supply chain from cyber events. It was developed in coordination with industry and academia and builds on previous standards including NIST 800-171, 800-53, CSF, ISO 27002, CIS v7 and Secure Controls Framework.

- **It is required for all organizations doing business with the DoD.** This is a sweeping change. If you work with the DoD, it applies to you, your supply chain and your business partners.
- **There are five levels of compliance.** All businesses need some level of cyber protection, ranked from 1 (Basic) to 5 (Advanced). What level of certification does your business need?
- **Compliance at the appropriate level will be a requirement for bidding.** Contracts will specify the maturity level required for any bidder. If you are not certified at the right level, you will not be able to bid.
- **Certification must be done by a third party.** Businesses cannot claim to be at a certain level of compliance. CMMC requires formal certification by a third party.
- **COVID-19 disruption will not impact the timeline of this regulation coming into force.**

What can Control Risks do to help?

Control Risks can help you by providing a pre-audit review of your cyber program and offering a clear set of actions you will need to take to prepare for the auditors. Our expert consultants can assist you in implementing the required changes so you can approach the audit process with confidence. We bring our extensive experience conducting cyber security assessments to this new framework. Our practice has a proven record of guiding organizations across a host of sectors to develop and implement comprehensive, compliance and risk-based cyber security programs. We are well positioned to help you.

Control Risks' team of experts will:

- Work with you to determine an appropriate level of CMMC compliance for your business
- Assess the current state of your cyber security program against your risks and the CMMC standard
- Deliver explicit guidance to address the CMMC requirements in a manner that fits the business
- Support you in implementing the changes you need to make

Control Risks understands that compliance is not the same as security. Our experts can ensure your organization is both compliant and secure. Control Risks helps organizations implement a full cyber program lifecycle that reinforces itself over time, creating a stronger, better prepared and more resilient organization.

Connect with our CMMC expertise

Michael Rohrs, Principal – Cyber Security, Washington DC

- Leads Control Risks cyber consulting practice in the Americas
- Extensive experience in global information and technology risk, cyber security, crisis management, incident response, intelligence, and geopolitical analysis
- Email: michael.rohrs@controlrisks.com or cyberamericas@controlrisks.com
- Telephone: +1 202 449 3331

About Control Risks

Control Risks is a leading risk consultancy that assists clients in managing political, security and integrity risks worldwide. Since 1975 we have worked for over 5,500 clients in more than 130 countries, helping them to accelerate business opportunities and manage risks in complex and challenging environments. We have developed an unparalleled ability to bring order to chaos and reassurance to anxiety. We are committed to helping our clients build organisations that are secure, compliant and resilient in an age of ever-changing risk and connectivity.

Creating secure, compliant and resilient organizations

Resolving critical issues and crises

Delivering growth and opportunity