corsica technologies

A Guide to CMMC Compliance

When it comes to CMMC compliance and control standards, certification is a go/no-go affair. And with DoD contracts on the line, it's imperative to produce a hygienic cybersecurity environment the first time around.

Use this guide as an overview of compliance requirements related to CMMC, as well as a resource for best practices when it comes to finding a strategic partner to help guide you through CMMC compliance regulations.

Why Should I Work Towards Compliance?

- Reduce your company's risk of cyberattack and financial loss
- Achieve best-in-class process controls, standards, and cyber hygiene
- Increase your chances of winning contracts throughout the DoD network and beyond
- Low up-front investment

An Intro to CMMC

Cybersecurity laws and regulations like NIST 800-171, ITAR, and CMMC are put in place to ensure that organizations are taking the right steps to protect sensitive federal data. But what makes CMMC significant?

The Cybersecurity Maturity Model Certification (CMMC) is a training, certification, and third-party assessment program of cybersecurity put forth by the U.S. government. Its aim is to certify that organizations handling federal data can securely process and store Controlled Unclassified Information (CUI).

The framework, designed to increase cyber hygiene through maturation of practices and processes, has a significant impact on the $712 billion defense industry. The Department of Defense (DoD) estimates the roll-out of CMMC standards will affect 300,000 companies.

If your organization is looking to enter a contract with the DoD or anyone in the defense contract supply chain, you will need to achieve the CMMC certification. Make sure you're equipped for certification today.

So What Do the CMMC Standards Require?

The CMMC covers five maturity levels ranging from Basic Cybersecurity Hygiene to Advanced/ Progressive and includes a third-party certification requirement for levels 1, 3, 4, and 5.

These levels are assessed by CMMC Third-Party Assessment Organizations, or C3PAOs. Each level is cumulative and consists of a series of practices or security controls that add up with each higher level.

Some levels of coverage include:

- Asset management
- Business continuity and disaster recovery
- Change management
- Cloud security
- Compliance
- Configuration management
- Cryptographic protections
- Continuous monitoring
- Data classification and handling
- Endpoint security
- Human resources security
- Identification and authentication
- Incident response
- Information assurance
- Maintenance
- Mobile device management
- Network security
- Physical and environmental security
- Project and resource management
- Risk management
- Security operations
- Secure engineering and architecture
- Security awareness and training
- Technology development and acquisition
- Threat management
- Vulnerability and patch management

Interested in the full CMMC compliance requirements?
Click here to download our free checklist.

When Will the CMMC Requirements Affect My Business?

There's no escaping it – CMMC requirements are coming. Many experts expect that the CMMC standards will come into full effect by 2025, with a slower implementation phase involving select organizations in the years prior.

In the meantime, many organizations are operating under the guidance of the Interim Rule.

Where the Interim Rule Comes Into Play

The Interim Rule amends the Defense Federal Acquisition Regulation Supplement (DFARS) to support a phased implementation of the CMMC framework.

Under the Interim Rule, all contractors will be required to publish a score representing their NIST 800-171 compliance progress before they can receive a contract. In addition to the score, contractors must also publish a date by which all requirements will be implemented. These terms are expected to be in effect through September of 2025.

The Interim Rule functions to offer contractors a grace period. However, the longer an organization puts off bringing its cybersecurity practices up to CMMC standards, the longer it puts off certification once they elect to apply.

Even if your organization is compliant with NIST 800-171 now, beginning to work towards CMMC compliance is the best-case scenario for winning federal contracts now and in the future.

Terms at a glance

Cybersecurity Maturity Model Certification (CMMC)

A training, certification, and third-party assessment program of cybersecurity put forth by the U.S. government.

Defense Federal Acquisition Regulation Supplement (DFARS)

DoD specific supplement to the Federal Acquisition Regulation. Contractors and subcontractors with the DoD must adhere to the regulations.

NIST-800-171

Publication that provides recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI).

Interim Rule

Ammends DFARS to support phased implementation of CMMC framework. Requires NIST 800-171 compliance and set date of full implenmentation.

The Benefits of CMMC Compliance

Reduce your company's risk of cyberattack and financial loss.

Aside from possible federal fines if your organization is breached, cyberattacks usually mean, at a minimum, a pause in business operations and a loss in subsequent revenue.

By certifying your organization to the CMMC standard, you reduce your risk of data breaches and other expensive cybersecurity incidents.

Achieve Best-in-Class Process Controls, Standards, and Cyber Hygiene

Certifying your organization to the CMMC standard does more than allow you to work with CUI and federal data. Meeting CMMC certification requirements puts your company in a great position to pursue certification in other regulations, including National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Modernization Act (FISMA), and Sarbanes-Oxley Act (SOX).

Low Up-Front Investment

Your exact initial investment depends on the desired maturity level and the size of your company. The good news is that the cost of the certification is allowable and reimbursable, meaning the upfront expense and any remediation costs can be billed to the DoD.

That means once your organization is certified to the CMMC standard, your organization can begin securely processing CUI and receive an immediate return on investment in the form of allowable expenses and increased opportunity for contracts.

Increase Your Chances of Winning Contracts Throughout the DoD Network and Beyond

Becoming CMMC certified gives your company a sharp competitive edge over non-CMMC certified competitors—even beyond winning government contracts. To the private sector, a CMMC certification shows that your company is trusted by the DoD and that you have gone above and beyond the minimum cyber standards. With a CMMC certification, your company is building trust throughout the DoD network as well as up and down your entire supply chain.

Working With a Registered Provider Organization (RPO) to Achieve CMMC Compliance

So, what are your first steps towards achieving CMMC compliance?

We recommend finding the right strategic partner to streamline your compliance efforts and guide the way. That means working with a Registered Provider Organization (RPO).

RPO approval from the CMMC Accreditation Body (CMMC-AB) reflects that a strategic partner is knowledgeable about the constructs of the CMMC standards and can deliver security services designed to help organizations with audits and meeting ongoing compliance requirements.

For your company, working with an RPO lessens the individual burden of navigating CMMC requirements on your own. Since an RPO undergoes training aligned with specific DoD expectations, it knows how to guide your organization's CMMC certification to success.

The Bottom Line?

CMMC certification is necessary for winning future contracts with the DoD. As an approved RPO, Corsica Technologies can help your organization build a more secure cyber environment, build trust throughout your supply chain, and help you win more contracts in the future. Pass your CMMC audit with confidence.

Click here to get started on the path towards CMMC compliance today.

About Corsica Technologies

Consistently recognized as one of the top managed IT and cybersecurity providers, Corsica Technologies helps organizations leverage technology as a competitive business advantage. Our integrated IT and cybersecurity services protect companies and enable them to succeed.

Accelerating Your Business Success.

sales@corsicatech.com (855) 411-3387 corsicatech.com

corsica technologies