CMMC READINESS CHECKLIST

Cybersecurity Maturity Model Certification (CMMC) compliance is required for organizations supporting DoD contracts starting in 2021. The new CMMC framework is a collection of the best practice control frameworks in use today, including NIST 800-171, ISO 9000, CMMI, RMF, and FedRAMP. DoD Requests for Proposals (RFPs) will require CMMC compliance and will be a prerequisite to enter the bidding process.

THE 5 LEVELS OF CMMC

The DoD structure contracts by their risk profiles. Each RFP will have a specific level requirement ranging from 1 to 5. To submit a bid, you'll need to have proof of certification.

LEVEL 1

Performed

17 controls must be applied. Every DoD contractor is required to complete these tasks.

LEVEL 2

Documented

72 controls must be applied (includes Level 1). This includes documentation to processes, such as SOPs, policies, and plans.

LEVEL 3

Managed

130 controls must be applied (includes Level 2).

LEVEL 4

Reviewed

156 controls must be applied (includes Level 3).

LEVEL 5

Optimzed

171 controls must be applied (includes Level 4).

Lower levels 1 and 2 apply to contractors who do not handle CUI (the majority of resellers). They will apply to contractors who do not keep government information on their corporate networks, except for HR data and purchase orders. Middle levels 3 and 4 are for DoD contractors who deal with CUI, and the highest levels 4 and 5 involve CUI that is highly sensitive and could include information on weapons tests or manufacturing schematics.

CMMC READINESS CHECKLIST

Regardless of level, there are 7 key steps to preparing for a CMMC certification:

□ **Task #1** | Define CUI Specific to the Contract and Identify Where CUI is Stored, Processed, and Transmitted

The US Government defines CUI for the prime contractor and the prime contractors is required to identify CUI in contracts to their subcontractors. Your initial task is to identify the CUI environment. These are the places in your facility where CUI is stored, processed, and transmitted.

□ **Task #2** | Identify Applicable CMMC Controls

Once you define the CUI environments, you can identify applicable CMMC controls with which your systems, services, and processes must comply.

□ **Task #3** | Create Policies, Standards, Guidelines, and Procedures

Rules provide for the protection of information and are commonly achieved through information security policies, standards, and procedures.

Information Security Policy consists of high-level statements relating to the protection of information across the business and should be produced by senior management.

Standards consist of specific low-level mandatory controls that help enforce and support the Information Security Policy.

Guidelines are recommended non-mandatory controls that support standards or serve as a reference when no applicable standard is in place.

Procedures consist of step-by-step instructions to assist workers in implementing the various policies, standards, and guidelines.

Documentation is critical to compliance and requires you to clearly write out a hierarchical structure that includes policies, standards, and procedures. Documents should be clear, follow a logical order, and have identifiable delineation of all compliance requirements. Every contractor is in a unique situation, and preparation begins by determining the compliance landscape in which your organization operates, including:

- **Domestic and international cybersecurity and privacy laws**
- **Industry-specific regulations**
- **Legally binding contracts**

□ **Task #4** | Operationalize the Policies & Standards to Implement CMMC Controls

By applying CMMC controls to your policies and standards, you determine what you will need to do to achieve and maintain CMMC compliance.

□ **Task #5** | Document the CUI Environment

This task identifies gaps preventing compliance with the CUI environment and its controls. The goal is to document these gaps in two primary documents:

System Security Plan (SSP) provides an overview of the security requirements for the CUI environment and describes the security controls in place and planned to meet those requirements. It includes information on the people, technology solutions, and processes contained within the CUI environment.

Plan of Action & Milestones (POA&M) will highlight CMMS control deficiencies. If you want to pass a CMMC audit, these documents must be completed in full detail. One of the very first things a CMMC auditor will request is access to both files. Failure to do so will likely end in an automatic non-compliance decision.

□ **Task #6** | Leverage the Controls to Assess Both Risk and Maturity Across Technology & Business Processes

There are various ways to assess risk. CMMC mentions NIST 800-37, ISO 31010, OCTAVE, and FAIR methodologies. CMMC wants to ensure you are measuring risk and taking steps to mitigate it by applying controls.

□ **Task #7** | Utilize Metrics from Control Execution to Identify Areas of Improvement

Once controls are established, you need metrics to demonstrate control effectiveness, progress towards achieving identified areas of improvement, and optimization. Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) related to you organization should be established and monitored.

GET PREPARED WITH CONCORD SECURITY

CMMC was created to establish clear guidelines and audit frameworks for contractors working with the DoD. In the months ahead, more information will be available, detailing the specifics of CMMC audits and frameworks. For now, all you can do is start preparing. This starts with the implementation of Level 1 controls. Noticeably, CMMC only details what practices companies must implement, now how it should be done.

CONCORD'S SECURITY EXPERTISE

Concord thoroughly understands all of the controls that will inform CMMC compliance and can help you prepare for a CMMC audit, no matter what level of certification you seek. We have the necessary processes and templates to undertake a gap analysis and create your overall security plan, plus the resources and expertise to complete remedial activities, if required. Further, we have tools to monitor security performance, resolve issues, and provide detailed reporting. As a result, Concord's expertise and toolsets can save you significant time and money.

Reach out today to secure your business and land those DoD contracts!