CYBERSECURITY PROFESSIONAL SERVICES

Cybersecurity Maturity Model Certification (CMMC)

The CMMC establishes five certification levels that reflect the maturity and reliability of a company's cybersecurity infrastructure.

MorganFranklin CONSULTING
A Vaco Company

PREPARE FOR UPDATES TO CMMC COMPLIANCE

The DoD plans to slowly roll out CMMC compliance requirements for new contracts beginning in 2021 with the expectation that every active contract will have a CMMC level requirement in place by 2026. The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing cybersecurity across the defense industrial base (DIB), which includes over 300,000 companies in the supply chain doing business with government agencies.

APPLICABILITY

All DoD contractors will eventually be required to obtain a CMMC certification. This includes all suppliers at all tiers along the supply chain, small businesses, commercial item contractors and foreign suppliers. The CMMC Accreditation Body (CMMC-AB) will coordinate directly with DoD to develop procedures to certify independent Third-Party Assessment Organizations (CP3AOs).

CMMC MATURITY LEVELS

The CMMC covers 5 levels of certification based on cybersecurity maturity. All levels above Level 1 consist of two measurements; Processes and Practices. Processes are things such as creating policies and plans for each of the 17 domains covered by the CMMC. Practices are the actual implementation of controls such as Access Control and Configuration Management.

CERTIFICATION READINESS

Our approach is centered around assisting our clients to understand current state maturity levels, determining the appropriate target state, identifying gaps from current state to target state, and developing a strategy and roadmap to close gaps and enhance controls in preparation of CMMC certification.

CERTIFICATION PROCESS

As companies are not allowed to self-certify under the CMMC, they must be audited by a certified third-party assessment organization (C3PAO) or a credited individual assessor to achieve compliance. C3PAOs provide advisory services, schedule the assessments, hire and train individual assessors, and review the results with the CMMC-Accreditation Body (AB) Quality Auditors.

READINESS ASSESSMENT AND SUPPORT

MorganFranklin is a **Registered Provider Organization (RPO)** certified by the CMMC Accreditation Body to guide organizations through the process of achieving CMMC compliance.

We follow a three-step Readiness Assessment to identify and close the gaps between an organization's current security posture and their target level of CMMC compliance.

1. Planning and Discovery
2. Readiness Assessment and Gap Analysis
3. Strategy and Roadmap

Compliance Support Services

In addition to performing a Readiness Assessment, we also offer support to organizations looking to carry out their CMMC Roadmaps.

MorganFranklin has deep expertise in selecting and deploying solutions to meet compliance requirements, and our Managed Security Services offerings can help to fill identified security gaps.