CMMC GAP Assessment

The Cybersecurity Maturity Model Certification is a Department of Defense program built to protect the defense industrial base from cyber-attacks.

About CMMC

The Cybersecurity Maturity Model Certification (CMMC) is a major Department of Defense (DoD) program built to protect the defense industrial base (DIB) from increasingly frequent and complex cyber-attacks. CMMC specifically aims to enhance the protection of controlled unclassified information (CUI), and federal contract information (FCI) shared within the DIB.

CMMC assures the DoD that a DIB company can adequately protect sensitive CUI and FCI, accounting for information flow down to subcontractors in a multi-tier supply chain.

The Opportunity

The professionals at IntraSystems Advisory Divison bring their experience and CMMC Registered Practitioner (RP) training knowledge to Organizations Seeking Certification (OSC) as part of a contract engagement.

Individuals holding an RP designation can provide CMMC implementation consulting services to assist in identifying gaps and providing mitigation strategies for an OSC preparing for an assessment.

How Can IntraSystems Advisory Divison Help?

While the process of CMMC Certification may seem complex and intimidating, IntraSystems Advisory Divison is here to assist with enhancing your security profile and preparing your organization for CMMC Compliance.

CMMC is expected to begin its initial rollout in 2023, with full implementation likely completed in 2025.

- Gap Assessment Services
- Final Certification Gap Remediation
- Support Across All Three CMMC Levels

CMMC Maturity Levels

The CMMC Framework requires a systematic approach to certification mapped to three organizational maturity levels: Foundational, Advanced, and Expert.

1 Level 1 Foundational

An organization must demonstrate basic cyber hygiene practices, such as ensuring employees change passwords regularly to protect Federal Contract Information (FCI). FCI is information not intended for public release provided by or generated for the government under a contract to develop or deliver a product or service to the government.

2 Level 2 Advanced

An organization must have an institutionalized management plan to implement good cyber hygiene practices to safeguard CUI, including all the NIST 800-171 r2 security requirements and processes.

3 Level 3 Expert

An organization must have standardized and optimized processes and enhanced practices to detect and respond to changing tactics, techniques, and procedures (TTPs) of advanced persistent threats (APTs). An APT is an adversary with sophisticated levels of cyber expertise and significant resources to conduct attacks from multiple vectors. Capabilities include having resources to monitor, scan, and process data forensics.

> The sooner clients implement practices to meet cybersecurity requirements, the better. Consistently performing processes to support these requirements will reduce the risk of non-compliance in an assessment. Keep in mind this is not a one-time exercise. Clients must self-assess and affirm compliance annually. Continuous monitoring, reviewing, and adjusting procedures are required to maintain compliance.

Benefits of the IntraSystems Advisory Divison Approach

Maximize Focus

Enable focus on initiatives that matter via a business- aligned IT strategy and executable roadmap.

Justify Strategy

Develop business cases with detailed BAU and target-state financial models.

Purposefully Execute

Equip your team with a detailed architecture and implementation plan, with resources to execute.

Ensure Adoption

Drive the success of the program via organizational change management.