CMMC Gap Assessment

Solution Brief

CMMC Gap assessment for manufacturing

The Department of Defense now requires contractors to obtain CMMC certification. The consequences of failing to do so are dire, including being ineligible for contracts, losing access to classified information, and facing significant penalties and fines. The question is, are you prepared?

About CMMC

In the complex landscape of cyber threats, CMMC certification is now a mandatory requirement for DoD contractors. The Cybersecurity Maturity Model Certification (CMMC) is a major Department of Defense (DoD) program built to protect the defense industrial base (DIB), including the manufacturing and energy sectors, from cyber attacks. CMMC aims to enhance the protection of controlled unclassified information (CUI) and federal contract information (FCI) shared within the DIB. By obtaining CMMC certification, contractors assure the DoD they have taken the necessary steps to protect sensitive Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

This includes the distribution of information to subcontractors in a multi-tier supply chain. The urgency to act cannot be overstated, as failure to comply can lead to the loss of contracts and business opportunities.

The Opportunity

For those seeking CMMC, IntraSystems Advisory Divisonprofessionals holding an RP designation can help manufacturers prepare for assessment, ensuring they adequately protect sensitive information and meet DoD requirements.

How Can IntraSystems Advisory DivisonHelp?

The process of obtaining CMMC Certification may seem overwhelming, but IntraSystems Advisory Divisonis here to help. Our team of experts can assist your organization in enhancing your security profile and preparing for CMMC Compliance.

CMMC is expected to begin its initial rollout in 2023, with full implementation likely completed in 2025, making it essential for organizations to take immediate action for compliance.

- 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 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.

Achieving compliance is not a one-time exercise.

Contractors must conduct self-assessments and affirm compliance annually to maintain their standing as a trusted partner of the Department of Defense. Continuous monitoring, reviewing, and adjusting procedures are necessary to ensure ongoing 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 as part of digital transformation.

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.

CMMC supports and accelerates digital transformation initiatives by helping improve security posture, mitigate cyber risk, and strengthen supply chain security. CMMC is an ecosystem-wide approach that helps create a more secure and reliable digital environment for defense-related projects.

Phone 781-986-1700 | info@intrasystems.com | www.intrasystems.com

intra systems Advisory Division