CMMC

Safeguarding sensitive information with the most advanced cybersecurity standards.

Cybersecurity Maturity Model Certification (CMMC) is a new compliance framework that will be required for all DoD contractors in the near future. It's overseen by the Office of the Under Secretary of Defense for Acquisitions and Sustainment (OUSD(A&S)) and establishes controls to meet security requirements set out in the Defense Federal Acquisition Regulation Supplement (DFARS). These controls are derived from NIST Special Publications (SP) 800-171 and 800-172.

CMMC 2.0 is the next iteration of the Department's CMMC cybersecurity model. It streamlines requirements to three levels of cybersecurity – Foundational, Advanced and Expert – and aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards.

Preparing for CMMC 2.0 with Technology Group Solutions

TGS has CMMC-AB Registered Practitioners on staff.

Registered Practitioners are training and tested against the Levels based on the CMMC Framework to obtain their designation. They are implementers that are providing consultative preparation services to the Organizations Seeking Certification (OSC).

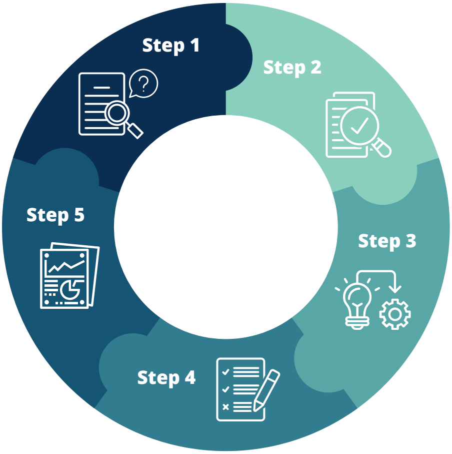
Our team will work with DoD and OSC contractors to help you meet the CMMC requirements. Organizations at Levels 2 and 3 will need third-party or government assessments on an annual or triennial basis. Technology Group Solutions will assess readiness and install or augment cyber security architecture to prepare for future C3PAO assessments, long-term certifications, and DoD contracts.

913-451-9900 | tgs-mtc.com | cmmc@tgs-mtc.com

Achieving CMMC Compliance: The Process

1. Prepare and Review

Implementation begins with a readiness assessment. OSC must determine the level of certification is required (Level 1-2); identify what sensitive information (FCI/CUI) needs to be protected, the current environment, what controls are currently in place, and how well these controls meet CMMC 2.0 requirements.



2. Analyze

Validate scoping criterion, documenting any deficiencies, and driving solutions to remedy identified issues (people, process, technology) to achieve objectives required b respective CMMC practices.

3. Implement

Identified strategies will be managed until OSC fully assimilate solutions. During the implementations phase, visibility with a dynamic GRC Platform (or other tool) is essential for visibility, tracking and status updates.

4. Audit

After controls have been implemented, an organization can begin the process of assessment and reporting, self-led or with a C3PAO or government agency facilitator (at CMMC Levels 1, 2, or 3, respectively).

5. Manage

CMMC implementation is an ongoing process, with re-assessment required at either annual or triennial increments. Periodic gap assessments, penetration testing, and patch management ensure that official certifications are streamlined and straightforward.

About Technology Group Solutions

TGS is a team of dedicated technology experts, community leaders, teachers, and advocates. We're more than an IT solutions provider. Our business is built on relationships, and since 2005, we've helped shape the way businesses approach IT by providing solutions that help our clients become more efficient, more accountable, and more profitable.

Our CMMC 2.0 services include readiness assessments and preparatory implementation. TGS will prepare your organization for CMMC 2.0 and all future versions of the CMMC. Contact us to schedule a consultation and rethink your approach to CMMC implementation.