RSI | Datasheet

CMMC

2.0 Implementation

Cybersecurity Maturity Model Certification (CMMC) is a compliance framework that ensures the cybersecurity practices of all DoD contractors align with the Department of Defense (DoD) requirements for handling Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). CMMC certification will begin appearing in contracts in 2025, with full compliance required by 2028. 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.

A CMMC Assessment validates that organizations in the Defense Industrial Base (DIB) comply with the DoD's cybersecurity standards. It ensures these companies have implemented and are effectively managing the security practices necessary to protect FCI and CUI, strengthening overall supply chain security. Assessments are conducted at different levels, ranging from Level 1 (Foundational) to Level 3 (Expert), based on the sensitivity of the information handled and the required security controls.

Preparing for the New CMMC with RSI Security

RSI Security has been approved by the Cyber-AB (formerly known as the CMMC-AB) as a Certified Third Party Assessment Organization (C3PAO), a Registered Provider Organization (RPO), and has technicians recognized as Registered Practitioners (RP). Our team has successfully assisted DoD contractors with NIST and DFARS compliance before the CMMC's rollout and has been working with CMMC clients since the rollout began.

With the new 2.0 protocols, most organizations at Levels 2 and 3 will need third-party or government assessments on an annual or triennial basis. RSI Security will assess readiness and install or augment cybersecurity architecture to prepare for future CMMC assessments, long-term certification, and DoD contracts. As a C3PAO, we also perform certified assessments.

What Does CMMC Require?

CMMC 2.0 comprises of 3 Levels:

Level 1: Foundational (17 Practices)

Level 2: Advanced (110 Practices)

Level 3: Expert (110+ Practices)

Your organization's contract will specify which Level is required. Level 1 is aligned with basic safeguarding of FCI. Level 2 adds on requirements for handling CUI and includes all of NIST SP 800-171. Level 3 includes the requirements of the previous two levels as well as a selection of controls from NIST SP 800-172.

RSI Security's CMMC Advisory

RSI Security's CMMC services provide a comprehensive readiness assessment to support the implementation and documentation of controls at any CMMC 2.0 Level. Our services also include:

- Identification of in-scope assets and systems handling CUI/FCI
- Review of documentation that assesses policies, procedures, and governance frameworks.
- Technical testing including internal and external penetration testing, vulnerability scans, and configuration reviews.
- Gap analysis highlighting areas of non-compliance and weaknesses.
- Remediation plan with actionable recommendations to address any gaps.

Achieving CMMC Compliance: The Process

1. Prepare and Review

Implementation begins with a readiness assessment. DoD contractors must determine what sensitive information needs to be protected, what controls are already in place to protect it, and how well these correspond to NIST SP 800-171 and SP 800-172 Requirements. The former primarily focuses on Controlled Unclassified Information (CUI), whereas the latter includes protections against Advanced Persistent Threats (APTs). Another consideration during the data gathering phase is which CMMC Level is currently required and which may be required later.

2. Implement

Following up on the readiness assessment, collected scoping data should be analyzed according to the CMMC Level required for the DoD contract. This allows the organization to determine which controls must be installed—and how—to meet all requirements while avoiding program overlap. All controls must be installed and documented.

3. Assessment

After controls have been implemented, an organization can begin the assessment and reporting process, either self-led or facilitated by a C3PAO or government agency (at CMMC Levels 1, 2, or 3, respectively. This process includes reviewing documentation to verify compliance with CMMC practices, performing technical evaluations and testing the organization's systems and networks, and conducting interviews and observations with key personnel to validate compliance.

4. Certification

After the assessment, the organization receives a certification of compliance or a comprehensive report detailing findings and areas of non-compliance. If the organization fails the CMMC assessment, they will need to undergo remediation to address the identified gaps in security practices and controls. This may involve revising policies, enhancing technical safeguards, and improving overall compliance with CMMC requirements. Once remediation efforts are complete, the organization can request a follow-up assessment to verify compliance and obtain the CMMC certification.

5. Continuity

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 recertifications are streamlined and straightforward.

RSI Security's GRC Tool: Your CMMC Management Solution

RSI Security's GRC Tool empowers seamless management of your CMMC 2.0 implementation, along with all other governance, risk, and compliance (GRC) needs. Highlights of the platform include:

- Provides pre-built templates for CMMC and other common frameworks like SOC 2, ISO, and NIST
- Automates repetitive and time-consuming tasks such as data gathering, documentation, and reporting
- Step-by-step verification for every CMMC requirement
- Integrates with popular tools like Slack, G Suite, and Microsoft 365 for seamless communication and data flow
- Enables real-time collaboration with team members and clients
- Tracks, assesses, and mitigates risks with intuitive dashboards and comprehensive reporting

About RSI Security

RSI Security is an approved C3PAO and Registered Provider Organization by the Cyber-AB, with technicians recognized as Registered Practitioners. Our comprehensive CMMC 2.0 services include readiness assessments, implementation guidance, and certified assessments. Leveraging years of experience in helping contractors meet NIST and DFARS compliance, we ensure your organization is prepared for CMMC 2.0 and future iterations. Contact us today to schedule a consultation and take the next step in securing your path to CMMC compliance.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com