RSI | *Datasheet*

CMMC

2.0 Implementation

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.

In November 2021, the DoD announced the launch of CMMC 2.0, a significant overhaul of the framework. CMMC 2.0 is intended to streamline implementation, but working with an advisory partner remains the best way to ensure swift, seamless certification.

Preparing for the New CMMC with RSI Security

RSI Security has been approved by the CMMC Accredidation Body (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 3 Levels, unlike the prior version, which had 5. The new Levels are:

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 2 includes all of NIST SP 800-171, whereas Level 3 is based on a selection of controls from NIST SP 800-172.

RSI Security's CMMC Advisory

RSI Security's CMMC services include:

- CMMC readiness assessment for implementation and documentation of controls, at any CMMC 2.0 Level
- A comprehensive GRC platform to empower visibility, tracking, and reporting from one central hub
- Mapping to NIST, DFARS, and other applicable regulatory frameworks
- Internal and external penetration testing and vulnerability scans for compliance

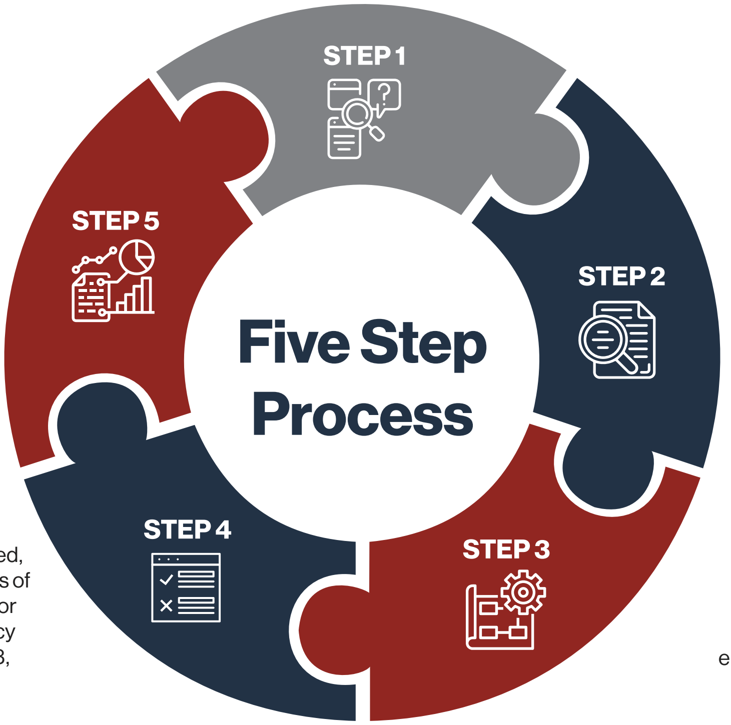
Achieving CMMC Compliance: The Process

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.

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 recertifications are streamlined and straightforward.



2. Analyze

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.

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).

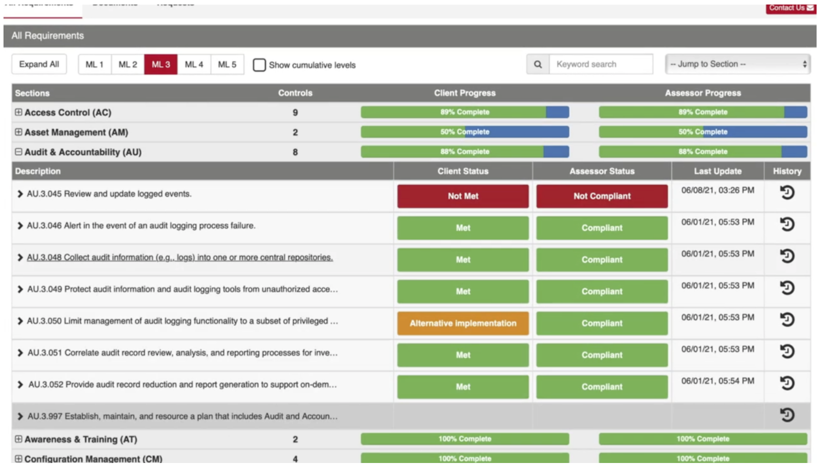
3. Implement

Following up on the readiness assessment, all controls must be installed and documented. A GRC platform, such as Redwood Portal, enables visibility over implementation and update status.

Redwood Portal: Your GRC Management Solution

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

- Implementation and update status visibility
- Workflow management and reporting via cloud
- Step-by-step verification for every requirement
- Robust communication and collaboration
- Secure data storage



Sections	Controls	Client Progress	Assessor Progress
⊞ Access Control (AC)	9	89% Complete	89% Complete
⊞ Asset Management (AM)	2	50% Complete	50% Complete
⊟ Audit & Accountability (AU)	8	88% Complete	88% Complete

Description	Client Status	Assessor Status	Last Update	History
› AU.3.045 Review and update logged events.	Not Met	Not Compliant	06/08/21, 03:26 PM	⟲
› AU.3.046 Alert in the event of an audit logging process failure.	Met	Compliant	06/01/21, 05:53 PM	⟲
› AU.3.048 Collect audit information (e.g., logs) into one or more central repositories.	Met	Compliant	06/01/21, 05:53 PM	⟲
› AU.3.049 Protect audit information and audit logging tools from unauthorized acce…	Met	Compliant	06/01/21, 05:53 PM	⟲
› AU.3.050 Limit management of audit logging functionality to a subset of privileged …	Alternative implementation	Compliant	06/01/21, 05:53 PM	⟲
› AU.3.051 Correlate audit record review, analysis, and reporting processes for inve…	Met	Compliant	06/01/21, 05:53 PM	⟲
› AU.3.052 Provide audit record reduction and report generation to support on-dem…	Met	Compliant	06/01/21, 05:54 PM	⟲
› AU.3.997 Establish, maintain, and resource a plan that includes Audit and Accoun…				⟲

Sections	Controls	Client Progress	Assessor Progress
⊞ Awareness & Training (AT)	2	100% Complete	100% Complete
⊞ Configuration Management (CM)	4	100% Complete	100% Complete

About RSI Security

RSI Security has been approved by the CMMC-AB as a Certified Third Party Assessment Organization, a Registered Provider Organization, and has technicians recognized as Registered Practitioners. Our CMMC 2.0 services include readiness assessment, preparatory implementation, and certified assessments. With years of experience guiding contractors into NIST and DFARS compliance, we 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.