# Authorized C3PAO

***AI-powered insight. Human-led expertise.***
***Independent assessment. Objective results.***

## What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is a unified standard designed to safeguard sensitive information across the Defense Industrial Base (DIB). Overseen by the Department of Defense (DoD) Chief Information Ocer (CIO), CMMC streamlines requirements from multiple cybersecurity frameworks — primarily NIST SP 800-171 and 800-172—into three levels of increasing rigor.

All organizations that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) for DoD contracts will need to achieve and maintain the appropriate CMMC level. These requirements are built into the Defense Federal Acquisition Regulation Supplement (DFARS), making compliance essential for contract eligibility.

## Benefits of CMMC 2.0

Being CMMC 2.0 compliant oers more than just access to Department of Defense contracts — it also strengthens your organization's cybersecurity posture, builds trust with partners, and reduces risk. It's a smart move for any business in the defense supply chain and a competitive edge for those in adjacent industries.

- Boosts credibility and trust
- Strengthens protection against cyber threats
- Reduces legal, financial, and reputational risk
- May lower cyber insurance premiums

## Compliance Requirements

CMMC requirements are incorporated into applicable DoD contracts through DFARS 252.204-7021. Beginning in 2025, CMMC requirements will be phased into solicitations, with broader enforcement continuing over subsequent years.

Organizations that store, process, or transmit FCI or CUI may be required to demonstrate the appropriate CMMC level based on contract scope and data sensitivity. Failure to meet required CMMC levels may result in contract ineligibility or loss of award eligibility.

## RSI Security is an approved C3PAO

RSI Security is an authorized Certified Third-Party Assessor Organization (C3PAO) accredited by Cyber AB to perform CMMC Level 2 assessments. In this role, RSI Security conducts independent, impartial assessments in accordance with the CMMC Assessment Process (CAP) and Department of Defense requirements.

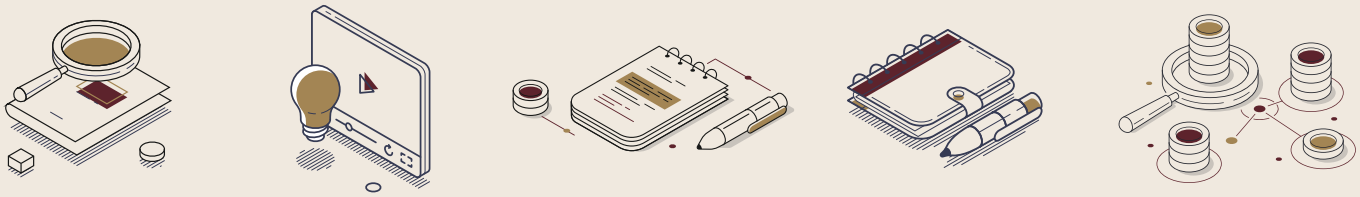
To maintain assessor independence, RSI Security does not provide CMMC advisory, implementation, remediation, or tool-selection services to organizations it assesses.

### CMMC Assessment Scope Includes:

- Independent evaluation against CMMC Level 2 assessment objectives
- Review of documented policies, procedures, and technical controls
- Interviews with personnel responsible for control operation
- Sampling and validation of objective evidence
- Formal assessment reporting aligned with CMMC requirements
- Assessment results subject to internal quality review

## RSI Security's 5-Step CMMC Process

RSI Security performs CMMC assessments solely in its capacity as an authorized C3PAO. RSI Security does not provide advisory, readiness, implementation, remediation, or tooling services to organizations it assesses.



**Organizational Preparation**

Prior to engaging a C3PAO, organizations are responsible for completing internal preparation activities, including identifying applicable CMMC levels, implementing required controls, and ensuring relevant documentation and evidence are available for assessment.

**Control Implementation**

Organizations implement and operationalize required security controls in accordance with applicable CMMC and NIST requirements prior to scheduling an independent assessment.

**CMMC Assessment**

RSI Security conducts an independent CMMC assessment in its role as an authorized C3PAO. The assessment includes evaluation of objective evidence, interviews with designated personnel, and testing of applicable controls in accordance with the CMMC Assessment Process (CAP).

**Assessment Results**

Upon completion of the assessment and required quality reviews, the organization may achieve CMMC certification if all applicable requirements are satisfied. If deficiencies are identified, results are documented in accordance with CMMC reporting requirements.

**Ongoing Maintenance**

Maintaining CMMC status is the responsibility of the organization and includes continuous operation of required controls and completion of periodic reassessments in accordance with CMMC requirements.

**Ready to Take the Next Step?**

RSI Security conducts independent CMMC Level 2 assessments as an authorized C3PAO, providing objective evaluation in accordance with DoD and Cyber AB requirements.

858.999.3030 | info@rsisecurity.com | rsisecurity.com