PRESENTED BY RSI SECURITY

A Buyer's Guide to Choosing a CMMC Partner

How to Select the Ideal CMMC Advisory and C3PAO Partner for Long-Term Compliance Success

Version 1.0 | **Revised** JAN 2026

CHOOSING A CMMC PARTNER

Table of Contents

RSI Security operates advisory (RPO) and assessment (C3PAO) services as separate, independently governed business functions. Engagement in RSI advisory services does not influence assessment outcomes, assessor assignment, scoring, or certification decisions. Clients are under no obligation to select RSI Security as their C3PAO following advisory services and may engage any authorized C3PAO listed by the Cyber AB.

PART I

Executive Summary

Protecting the Defense Industrial Base begins with choosing the right compliance partner.

The Department of Defense's Cybersecurity Maturity Model Certification (CMMC) program establishes verifiable cybersecurity requirements for contractors handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The DoD is scheduled to begin incorporating CMMC assessment requirements into applicable procurements starting November 10, 2025, aligning with the effectiveness of the revised DFARS 252.204-7021. Implementation will then proceed in phases over multiple years per the CMMC Program rule at 32 CFR Part 170.

RSI Security bridges that gap—without compromising independence.

RSI Security is recognized in the CMMC ecosystem as both a Registered Provider Organization (RPO) and a Certified Third-Party Assessment Organization (C3PAO). Our advisory team prepares organizations to meet NIST SP 800-171 requirements—and SP 800-172 where applicable—helping teams document evidence effectively and sustainably. Independently, our assessment team conducts impartial Level 2 third-party assessments authorized by the Cyber AB, submitting validated results that underpin the Government's certification decision while strictly maintaining the required separation of duties.

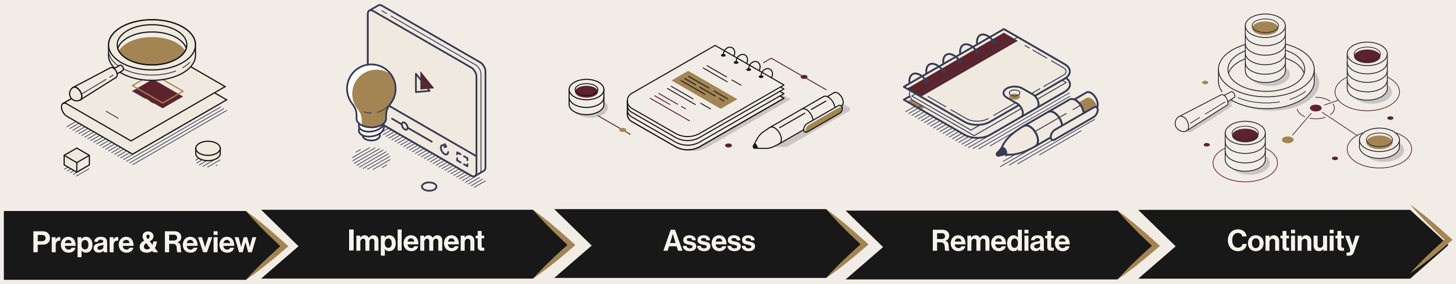
What you'll learn inside:

01 How to evaluate a qualified CMMC Advisor—including credentials, methodology, and tooling—against DoD expectations.

02 How to select a C3PAO assessment partner based on objectivity, transparency, and cross-framework rigor.

03 Practical tools—key questions, comparison matrices, and readiness checklists grounded in NIST SP 800-171/172 and DoD guidance.

04 How aligning readiness work to official CMMC assessment criteria can reduce rework, improve evidence quality, and support long-term compliance.



Prepare & Review

We begin with a readiness review to identify what requires protection, what controls already exist, and where gaps may appear.

Implement

We guide your team through implementing required practices, aligning controls to contract requirements, and documenting each action.

Assess

We support your assessment by validating evidence, reviewing documentation, conducting walkthroughs, and preparing your team.

Remediate

If gaps appear, we help you address them efficiently — updating policies, strengthening controls, and improving technical safeguards.

Continuity

We support continuous monitoring, periodic gap assessments, and security improvements so your organization stays ready for annual reviews.

CMMC compliance is more than a regulatory requirement—it's a strategic advantage.

Early, well-documented alignment to NIST SP 800-171 and a credible path to CMMC assessment protect contract eligibility, strengthen cyber resilience, and build trust across the Defense Industrial Base (DIB). RSI Security helps you get—and stay—there. Our proven frameworks, seasoned experts, and proprietary GRC tools make compliance achievable, repeatable, and scalable for every stage of your cybersecurity maturity.

PART II

Understanding the CMMC Landscape

Building cybersecurity resilience isn't just about defense—it's about eligibility, trust, and future-proofing your business.

The CMMC program is the DoD's formal, enforceable mechanism to verify contractor cybersecurity maturity when handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). In contrast to previous self-attestation models, CMMC introduces mandatory, structured assessments—ranging from self-attestation to independent third-party certification—aligned with tiered levels of risk and data sensitivity.

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's unified framework for protecting sensitive information across the Defense Industrial Base (DIB). With CMMC 2.0 nearing implementation, contractors must meet clearly defined security requirements to demonstrate they can safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

CMMC realigns contractor cybersecurity obligations into three levels and ties them to existing federal standards. Each level corresponds to increasing data sensitivity and maturity expectations.

CMMC includes three certification levels:

	Level 1 *Foundational*	Level 2 *Advanced*	Level 3 *Expert*
Purpose	Basic safeguarding of FCI	Protection of CUI	Highest-level protection (CUI + advanced threat)
Applicable Frameworks	15 practices From FAR 52.204-21	110 controls From NIST SP 800-171 Rev 2	Builds on 110 NIST SP 800-171 + selected NIST SP 800-172
Assessment Type	Annual self-assessment / Contractor (with senior official affirmation)	Level 2 (Self) or Level 2 (C3PAO) as specified in the contract solicitation.	Government led assessment
Who Performs the Assessment	Contractor	Accredited Certified Third-Party Assessment Organization (C3PAO) or self depending on contract	Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) or equivalent

Why CMMC Compliance Matters

Effective November 10, 2025, DoD solicitations will begin incorporating CMMC requirements (via the revised DFARS 252.204-7021) for applicable awards, marking the start of a phased implementation across the Defense Industrial Base. Failing to achieve or maintain the required CMMC level will result in ineligibility for new contract awards and may jeopardize option-year renewals.

Business value beyond compliance:

- Stronger protection against data breaches and insider threats.
- Becoming a verified partner boosts vendor credibility across the DIB.
- Aligning cybersecurity maturity can reduce risk, insurance premiums, and audit burdens.
- Demonstrating readiness positions you to respond to evolving DoD contract requirements and supply-chain risk

The Ecosystem: Who's Who in CMMC

Recognizing the roles of key entities helps you evaluate partners effectively:

Cyber AB (Accreditation Body)

Accredits C3PAOs and authorizes RPOs; oversees the ecosystem on behalf of DoD. Ensure your partner is listed in the Cyber AB Marketplace and referenced in 32 CFR 170.

Registered Provider Organization (RPO)

Provides advisory/readiness services (cannot issue certification). Provides advisory/readiness services (cannot issue certification).

DoD / DCMA / DIBCAC

Defines requirements, oversees high-risk assessments (Level 3). Keeps you informed of contract flow-downs and sourcing expectations.

Certified Third-Party Assessment Org

Authorized to perform Level 2 assessments and submit results to the CMMC Enterprise Mission Assurance Support Service (eMASS) for certification. Cyber AB listing, experience in assessments, independence.

**RSI Security holds dual recognition as both an RPO and C3PAO—enabling end-to-end support while maintaining strict separation of duties and independence as required by the CMMC rule.

How CMMC Connects to NIST and DFARS

CMMC draws directly from existing frameworks:

- FAR 52.204-21 governs 15 basic safeguarding practices for FCI (Level 1).
- DFARS 252.204-7012 mandates NIST SP 800-171 for CUI protections (foundation for Level 2).
- DFARS 252.204-7021 signals inclusion of CMMC status requirements in solicitations.
- NIST SP 800-172 supplies enhanced protections applicable to Level 3 assessments.

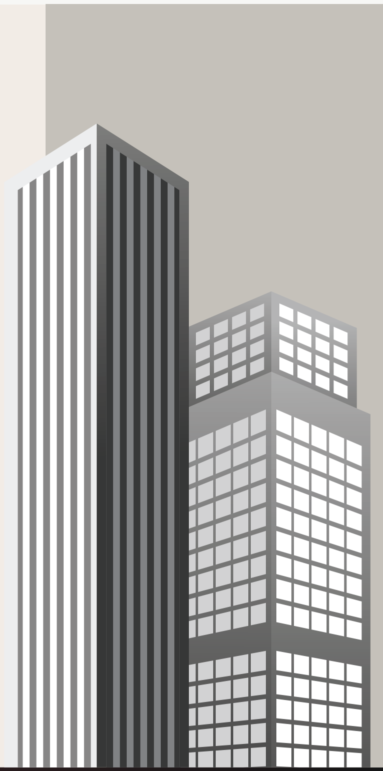
Thus, CMMC does not replace NIST or DFARS—it provides the verification and certification layer on top of them for DoD contracting.

Strategic Outlook

Cybersecurity is no longer just a cost—it's a competitive differentiator in DoD contracting. Contractors who proactively align with CMMC set themselves up for long-term success—while those who wait face potential contract rejection, accelerated remediation costs, and supply-chain exclusion.

With RSI Security's advisory-first model and certified assessment capability, your organization can accelerate readiness, approach assessment with confidence, and sustain maturity across the multi-year transition ahead.

Schedule a CMMC scoping workshop to define your boundary and readiness timeline before requirements hit.



PART III

The Guide to CMMC Advisory Partners

Choosing the right CMMC Advisory Partner is the single most important step in preparing for certification.

The Department of Defense now requires verifiable cybersecurity maturity as a condition of contract eligibility. Before an accredited C3PAO can assess your organization, you need a trusted advisor to help you interpret the standards, close gaps, and build an evidence chain that stands up to assessment scrutiny.

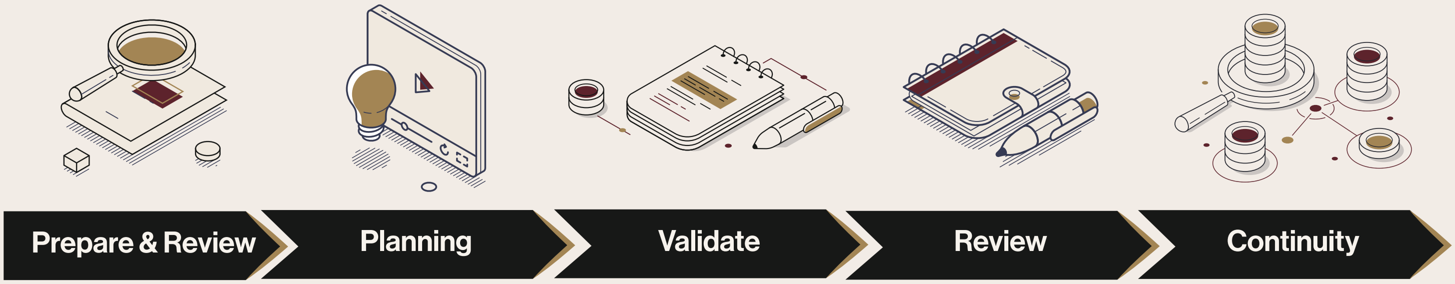
A qualified advisory partner does more than prepare documentation—they operationalize compliance by embedding security maturity into your business processes, systems, and culture.

The Role of a CMMC Advisory Partner

Advisory partners—specifically Registered Provider Organizations (RPOs)—are authorized by the Cyber AB to provide readiness and consulting services. They cannot conduct official certifications—that independence ensures objectivity during formal assessments.

An RPO's purpose is to help your organization:

- Interpret and apply NIST SP 800-171 Rev 2 (and, if applicable, SP 800-172) controls.
- Develop and document security policies, procedures, and implementation evidence.
- Create a System Security Plan (SSP) and Plan of Actions and Milestones (POA&M) aligned with DoD expectations.
- Build repeatable internal governance and reporting processes.



Prepare & Review

Objective: Define the CMMC Assessment Scope (Security Protection Assets, CUI Assets, etc.) and gather baseline documentation.

Activities: Identify in-scope systems, categorize FCI/CUI, and evaluate current control maturity.

Planning

Objective: Map controls and remediation priorities.

Activities: Conduct readiness assessment; develop POA&M; design roadmap aligned with CMMC Level requirements.

Validate

Objective: Execute control remediation and verify effectiveness.

Activities: Deploy technical safeguards, update policies, run tabletop exercises, and collect evidence.

Review

Objective: Conduct a Mock Assessment to simulate the C3PAO experience and validate objective evidence.

Activities: Internal review, documentation QA, and stakeholder training.

Continuity

Objective: Sustain compliance and prepare for future audits.

Activities: Annual gap reviews, vulnerability management, and live monitoring via RSI GRC platform.

This model directly mirrors DoD assessment methodology, ensuring readiness artifacts (SSP, POA&M, evidence) are organized in the format assessors expect.

What to Look For in a CMMC Advisory Partner

Not all consultants are equal—look for firms formally recognized by the Cyber AB and demonstrably fluent in DoD frameworks. Use this evaluation framework to guide your decision.

Authorization & Role Clarity

- □ Is the provider formally listed as a Registered Provider Organization (RPO) in the Cyber AB Marketplace?
- □ Do they clearly distinguish advisory/readiness services from independent assessment activities?
- □ Can they explain what advisory services do not include (e.g., certification, scoring, assessment)?

Remember:

Only authorized RPOs operate within the Cyber AB ecosystem. Clear role separation helps avoid conflicts of interest and preserves assessment integrity.

Framework Expertise

- □ Does the provider demonstrate practical experience with NIST SP 800-171 Rev. 2?
- □ Can they explain assessment objectives, not just control statements?
- □ Are they current on DoD guidance, including CMMC scoping and evidence expectations?

Why it matters:

Misinterpretation of NIST requirements is a leading cause of readiness gaps and POA&M rework during assessment.

Methodology & Structure

- □ Is there a documented, repeatable readiness approach aligned to CMMC assessment criteria?
- □ Are scope, evidence, and documentation addressed together—not as separate activities?
- □ Can the provider explain how readiness outputs map to what assessors evaluate?

Evidence Discipline & Tooling

- □ Does the provider emphasize objective evidence, not just policies and procedures?
- □ Is there a defined approach for organizing logs, records, configurations, and screenshots?
- □ Do they offer tooling or processes to manage evidence versioning and ownership?

Sustainability & Ongoing Readiness

- □ Does the approach support ongoing compliance, not just initial readiness?
- □ Are sustainment activities (e.g., gap refreshes, policy updates) clearly defined?
- □ Can the provider explain how organizations maintain posture between assessment cycles?

Final Buyer Tip

A qualified CMMC advisory partner should help you prepare responsibly, understand your obligations, and own your compliance posture—without influencing assessment outcomes or certification decisions.

The Power of RSI's GRC Tool

CMMC readiness requires accurate evidence management and cross-department coordination.

RSI's Governance, Risk & Compliance (GRC) Platform simplifies compliance operations by digitizing the entire lifecycle.

Core Capabilities:

- Pre-built CMMC templates mapped to NIST SP 800-171 Rev 2.
- Automated evidence collection and version control.
- Integration with Microsoft 365, Google Workspace, and Slack for collaboration.
- Risk registers and real-time dashboards for leadership visibility.
- Centralized document library for System Security Plans and POA&Ms.

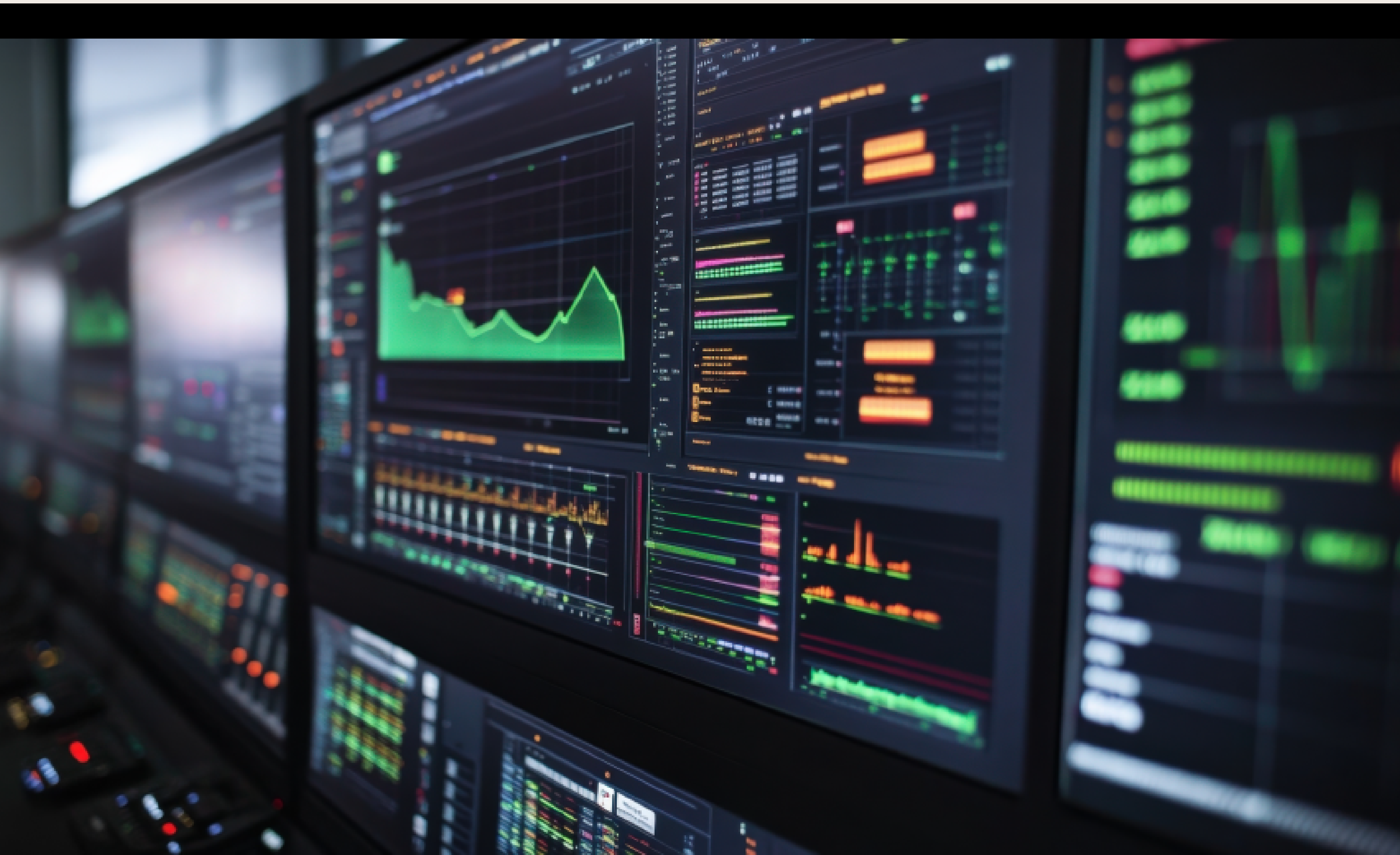
The Business Case for a Strong Advisory Partnership

Partnering with an authorized RPO is an investment in revenue continuity. The right advisor helps you:

- Protect revenue streams by maintaining DoD contract eligibility.
- Reduce assessment costs by minimizing remediation and rework.
- Strengthen security resilience against emerging cyber threats.
- Align compliance with business objectives, not just IT tasks.
- Establish a culture of continuous improvement through training and governance.

Certification is where readiness becomes reality. Once your organization completes CMMC readiness, the next step is a formal, accredited assessment.

Selecting the right Certified Third-Party Assessment Organization (C3PAO) ensures your evaluation is conducted according to DoD and Cyber AB standards—impartially, transparently, and efficiently.



PART IV

Guide to CMMC Assessment Partners

Certification is where readiness becomes reality.

Once your organization completes CMMC readiness, the next step is a formal, accredited assessment.Selecting the right Certified Third-Party Assessment Organization (C3PAO) ensures your evaluation is conducted according to DoD and Cyber AB standards—impartially, transparently, and with minimal operational disruption.

What is a C3PAO and Why It Matters

A C3PAO is an organization accredited by the Cyber AB and authorized by the Department of Defense to perform official CMMC Level 2 assessments.

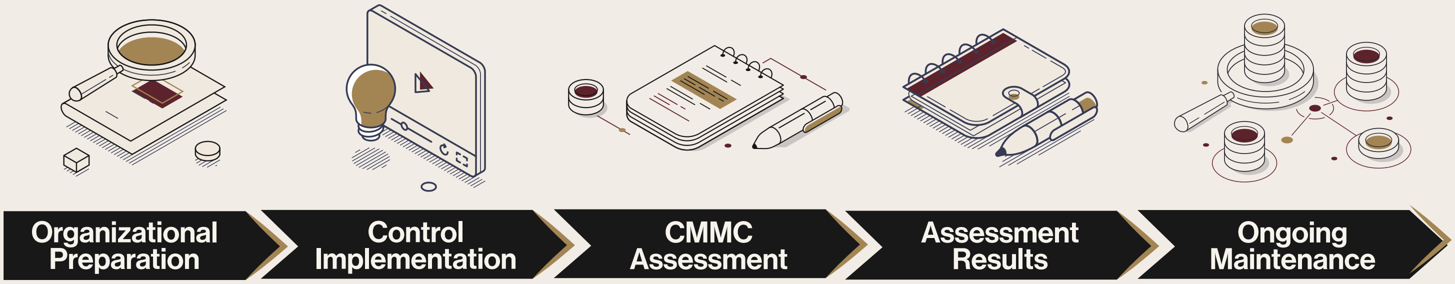
Only entities listed in the Cyber AB Marketplace are eligible to conduct third-party assessments that lead to certification recognition under DFARS 252.204-7021 and 32 CFR Part 170. C3PAOs operate under strict impartiality rules defined in the CMMC Rule—they strictly cannot provide advisory or remediation services for the same client engagement they assess.

This separation preserves the integrity and consistency of DoD's verification process.

RSI Security holds dual recognition as both an RPO and a C3PAO. These functions are maintained as independent business units, enabling RSI to deliver full-lifecycle support—from preparation to certification—while complying with Cyber AB impartiality requirements.

The CMMC Assessment Process Explained

The DoD prescribes a consistent, evidence-based process for all third-party assessments, described in the CMMC Assessment Guide (Level 2) and the CMMC Program Final Rule. A typical evaluation proceeds through five phases:



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.

Each phase is designed for traceability, repeatability, and transparency—core tenets of the DoD's assessment framework. Depending on organization size and documentation quality, most assessments span 6 to 12 weeks from initiation to Cyber AB validation.

What to Look For in a C3PAO Partner

When evaluating C3PAO candidates, confirm both formal accreditation and operational maturity. The table below provides a structured selection framework.

	Key Indicators	Why It Matters	RSI Security Advantage
Cyber AB Accreditation	Listed and active in Cyber AB Marketplace.	Only accredited C3PAOs may perform Level 2 assessments recognized by DoD.	RSI Security – Cyber AB-listed C3PAO authorized for Level 2.
Assessment Methodology	Uses DoD CMMC Assessment Guide (Level 2) and NIST SP 800-171 Rev 2.	Ensures uniform evaluation and scoring integrity.	RSI follows official DoD methodology end-to-end.
Objectivity & Impartiality	No consulting or remediation for same client.	Prevents conflict of interest preserves certification credibility.	RSI enforces strict separation of duties between advisory and assessment personnel.
Cross-Framework Expertise	Experience with DFARS, NIST, ISO 27001, SOC 2, etc.	Helps clients unify controls across frameworks.	RSI bridges multi-framework assurance programs.
Reporting Transparency	Clear communication pre-,during, and post-assessment.	Reduces misinterpretation and accelerates approval.	RSI provides status dashboards and structured report reviews.

Deliverables and What to Expect

A reputable C3PAO delivers actionable artifacts that enable clear certification decisions. Standard Deliverables:

- Assessment Plan – defines scope, systems, personnel, and data flows.
- Assessment Report – Documents findings for all assessment objectives across the 110 practices.
- Corrective Action Plan (POA&M) – Validates the closure of any allowable POA&M items (limited to specific controls) prior to final certification.
- Final Assessment Package – Uploaded to the DoD CMMC eMASS system for final review.
- Certification Notification – formal acknowledgment once validated by Cyber AB and DoD.

Maintaining Compliance After Certification

Under the CMMC Final Rule, organizations must maintain compliance continuously—certifications remain valid for three years at Level 2, subject to:

- Annual affirmations submitted by a Senior Company Official into the Supplier Performance Risk System (SPRS) confirming continued compliance.
- Spot audits or re-assessments if significant changes occur.
- Re-certification at three-year intervals through a C3PAO or DoD team.

PART V

Why Both Services Matter Together

CMMC success depends on more than technical controls—it depends on strategic alignment.

DoD's updated framework rewards organizations that can demonstrate not just compliance, but a sustainable cybersecurity culture. Advisory and assessment are distinct functions by design under Cyber AB policy—but when they are aligned through an integrated, impartial partner model, contractors move from reactive readiness to continuous resilience.

RSI Security is uniquely positioned to provide this dual-track advantage: we operate as both an authorized Registered Provider Organization (RPO) for preparation and an accredited Certified Third-Party Assessment Organization (C3PAO) for validation. Each function operates under strictly independent governance—preserving the objectivity required by the CMMC Program Final Rule while ensuring a seamless, consistent client experience.

Two Sides of the Same Mission

	Purpose	RSI Security's Role
Advisory (RPO)	Prepare organizations for certification by aligning with NIST SP 800-171/172 and DFARS 7012.	Conduct gap analyses, develop SSPs and POA&Ms, and perform mock assessments to validate readiness.
Assessment (C3PAO)	Independently verify that controls meet DoD and Cyber AB standards.	Perform authorized Level 2 assessments and submit validated results to DoD's eMASS system for certification.

Benefits of a Unified Partner Ecosystem

Working with disconnected vendors often introduces friction: duplicate evidence requests, inconsistent interpretations of controls, and prolonged timelines for certification. By contrast, RSI's integrated—yet strictly segregated—model delivers measurable advantages:

Aligned Methodology: Our readiness framework mirrors DoD's Assessment Guide structure, ensuring documentation produced during advisory maps directly to C3PAO evidence categories.

- **Accelerated Timelines:** Clients prepared under RSI's RPO process typically achieve C3PAO readiness with minimal remediation cycles—reducing the overall certification timeline.
- **Reduced Rework:** A standardized GRC infrastructure ensures your evidence, SSP, and POA&M are structured correctly for assessment consumption, minimizing format-based rejections.
- **Consistent Communication:** Dedicated project managers coordinate milestones across advisory and assessment teams for seamless transitions.
- **Sustained Compliance:** Continuous monitoring services maintain posture between annual affirmations and three-year re-certification cycles.

> ***"When readiness and certification share a common foundation, compliance becomes predictable—and cybersecurity becomes culture."***

The End-to-End Compliance Lifecycle

CMMC compliance is not a one-time milestone but an ongoing lifecycle of preparation, independent evaluation, and sustainment. Organizations typically begin with readiness activities—such as gap analysis, SSP development, and evidence organization—followed by an independent C3PAO assessment when required by contract. After certification, organizations must maintain compliance through annual senior official affirmations, continuous monitoring, and periodic reassessment at three-year intervals. Treating CMMC as a continuous improvement process helps organizations sustain cybersecurity maturity as requirements and threats evolve.

The RSI Security Difference

Dual Accreditation: Verified Cyber AB RPO + C3PAO, delivering full-spectrum capability while maintaining role independence.

Proven DoD Alignment: Methodologies derived from official CMMC Assessment Guides and NIST SP 800-171 Rev 2.

Technology-Enabled Oversight: Proprietary GRC platform for control mapping, evidence tracking, and audit readiness.

Defense Sector Experience: Trusted by primes and subs across aerospace, logistics, and advanced manufacturing.

End-to-End Continuity: From first readiness review to final certification and ongoing monitoring.

PART VI

Common CMMC Pitfalls

CMMC certification is rigorous. Unlike previous self-attestation models, a C3PAO assessment requires objective evidence that controls are functioning effectively. Below are the most common reasons organizations fail to achieve certification and how to prevent them.

Risk: Mis-Scoping the Environment

Many organizations either over-scope (increasing cost) or under-scope (hiding risks). A frequent error is failing to account for "Security Protection Assets" (SPAs)—tools like firewalls, MSPs, or SIEMs that don't store CUI but provide security for it.

The Fix: Map your data flows early. Ensure SPAs are fully assessed and that "Contractor Risk Managed Assets" are properly documented in your System Security Plan (SSP).

Risk: Over-Reliance on POA&Ms

Under the CMMC Final Rule, you cannot simply put hard-to-fix controls on a Plan of Actions and Milestones (POA&M) indefinitely. Critical controls (highest-weighted) must be fully met at the time of assessment, and any allowable POA&M items must be closed within 180 days.

The Fix: Treat the assessment as a "pass/fail" event for critical controls. Do not schedule your C3PAO assessment until high-value controls are fully implemented and validated.

Risk: "Paper" Compliance Without Evidence

Having a policy document is not enough. Assessors are required to verify that you are doing what the policy says. If your policy says "we review logs daily," but you lack 90 days of logs showing those reviews occurred, you will fail the control.

The Fix: Shift focus from writing policies to generating evidence. Automate log collection, ticketing for changes, and visitor logs to create an "audit-ready" trail of activity.

Risk: The "Shared Responsibility" Trap

Contractors often assume their Cloud Service Provider (CSP) or Managed Service Provider (MSP) handles compliance for them. However, if your MSP doesn't have a Shared Responsibility Matrix (SRM) defining exactly which controls they own versus which you own, gaps will inevitably appear during the assessment.

The Fix: Demand a CMMC-aligned Shared Responsibility Matrix from every IT vendor. Verify they hold the appropriate FedRAMP equivalency or CMMC certification for their role.

Outcomes vary by organization maturity, scope accuracy, and control implementation. No advisory engagement guarantees certification, scoring, or assessment results.

PART VII

Appendices

These reference materials consolidate verified DoD and Cyber AB information into actionable tools. Decision-makers can use them to benchmark readiness, interpret terminology, and navigate official resources while engaging RSI Security for expert support.

Key Terms Glossary

CMMC (Cybersecurity Maturity Model Certification): DoD's framework to verify that contractors implement required safeguards for FCI and CUI through independent assessment or affirmation.

C3PAO (Certified Third-Party Assessment Organization): Organization accredited by the Cyber AB to perform official CMMC Level 2 assessments recognized by DoD.

RPO (Registered Provider Organization): Cyber AB-authorized entity that provides CMMC advisory and readiness services but does not issue certifications.

NIST SP 800-171 / 800-172: Federal standards detailing 110 core controls (800-171) and enhanced protections against advanced threats (800-172).

FAR 52.204-21: Federal Acquisition Regulation clause requiring 15 basic safeguarding practices for FCI (Level 1 baseline).

DFARS 252.204-7012: Clause mandating implementation of NIST SP 800-171 for CUI and incident reporting to DoD within 72 hours.

DFARS 252.204-7021: The contract clause that implements CMMC requirements, requiring contractors to maintain the appropriate CMMC status for the duration of the contract.

Cyber AB (CMMC Accreditation Body): DoD-authorized entity that accredits RPOs, C3PAOs, and CMMC practitioners, maintaining the Marketplace directory.

SSP (System Security Plan): Comprehensive record of how each NIST SP 800-171 control is implemented within the organization.

POA&M (Plan of Actions and Milestones): Document listing unimplemented controls, associated risks, and timelines for remediation.

Annual Affirmation: A formal affirmation submitted annually by a Senior Company Official into SPRS, attesting to continuing compliance with CMMC requirements.

Three-Year Certification Cycle: Period of validity for CMMC certification (Level 2 or 3), requiring re-assessment every 36 months.

Additional Resources

DoD and Federal Resources

- CMMC Program Rule (32 CFR Part 170) — The regulation establishing the CMMC Program mechanics.
- DoD CMMC Program Website — Primary DoD reference for policy and FAQ updates.
- NIST SP 800-171 Rev 2 (Publication) — 110 required controls for CUI protection.
- NIST SP 800-172 (Publication) — Enhanced controls for advanced threat environments.
- Cyber AB Marketplace — Search for authorized RPOs and C3PAOs.

RSI Security Resources

- CMMC Advisory One-Sheet (2026) — Gap remediation and readiness planning overview.
- CMMC Assessment One-Sheet (2026) — Certified evaluation and certification pathway.
- CMMC Whitepaper (2026) — Quick-reference task guide for readiness validation.

☎ (858) 252-2448
(858) 225-6910

✉ info@rsisecurity.com
marketing@rsisecurity.com

🌐 rsisecurity.com
store.rsisecurity.com