

Expert CMMC Compliance

Guided Assessments, Workflows, and Audit Assurance.

PURPOSE

The primary purpose of CMMC is to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) by enforcing cybersecurity practices across the defense supply chain.

LEVELS OF MATURITY

CMMC defines multiple levels of cybersecurity maturity, ranging from basic to advanced. Levels correspond to specific security practices and processes. Organizations must achieve the required level based on their contract requirements and role in the supply chain.

ASSESSMENTS & CERTIFICATIONS

Organizations must currently self-assess their CMMC readiness. Once CMMC is fully implemented, organizations must undergo a CMMC assessment conducted by a CMMC Third-Party Assessment Organization depending on contractual requirements.

DOMAINS & PRACTICES

CMMC Level 1 covers 6 domains and 15 requirements. CMMC Level 2 covers 14 domains and 110 requirements that mandate more sophisticated cybersecurity defenses, including vulnerability management, incident response, and security awareness training.

CONTINUOUS IMPROVEMENTS

CMMC emphasizes continuous improvement and ongoing monitoring. Organizations must maintain their cybersecurity practices to retain their certification.

The Cybersecurity Maturity Model Certification framework was designed to enhance the cybersecurity posture of organizations that work with the US Department of Defense (DoD).

CMMC was established to safeguard sensitive information and ensure that contractors and subcontractors in the Defense Industrial Base (DIB) adhere to specific security standards. CMMC's requirements can be daunting for smaller defense organizations, but RADICL can help simplify the process.

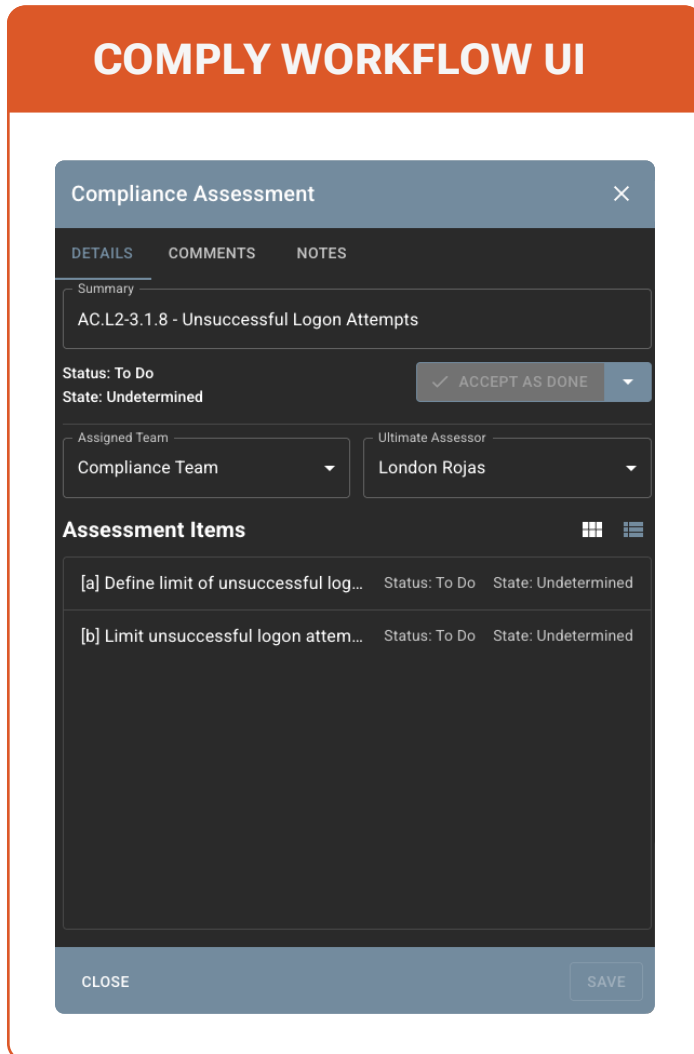
RADICL is a CMMC Registered Practitioner Organization (RPO) that was founded to protect DIB contractors through enterprise-grade cyberthreat protection and guided compliance adherence. CMMC provides a framework that can significantly improve an organization's cyberthreat resiliency while ensuring IT fundamentals are well in place.

RADICL removes the burden of managing the complex and confusing CMMC compliance process. Our intuitive platform provides advanced threat protection and addresses the hardest-to-meet CMMC Level 2 requirements, while ensuring motivated threat actors are deterred, detected, and stopped.

Our goal is to keep you truly secure while ensuring your CMMC compliance mandates are met, with minimal business interruptions, so that you can focus on serving your mission and customers.

TRANSFORMING UNCERTAINTY INTO CLEAR DIRECTION

Here's what RADICL's guided approach to CMMC compliance adherence looks like:



1. SCOPE ASSESSMENT

To start, we'll meet with your team for a series of workshops to understand and validate your compliance requirements and scope.

We'll strategize what can be done to reduce your in-scope infrastructure and operations in order to minimize compliance costs.

2. GUIDED SELF-ASSESSMENT

Our team periodically releases new assessments. The platform contains detailed implementation guidance and a complete suite of compliance policy and procedure templates that enable you to complete these assessments at a manageable pace.

3. REGULAR CHECK-INS

Our compliance experts will regularly meet with you to remove any doubts and continue to drive progress forward.

4. ASYNCHRONOUS SUPPORT

Communication tools integrated into our platform ensure that help is never far away.

We will do whatever we can to help your team quickly close gaps.

5. ASSESSMENT READINESS

Consultants will thoroughly review your submission so you can go into your assessment feeling confident and well prepared.



RADICL helps simplify, accelerate, and reduce the cost of CMMC compliance.



Visit radicl.com to learn more.

WHY SHOULD YOU TRUST RADICL FOR YOUR CMMC COMPLIANCE JOURNEY?

- **ADVANCED THREAT PROTECTION**

Squashing cyberthreats is what we do. In addition to ensuring that you're compliant, we'll keep you safe from motivated threats that seek to steal your data, disrupt your operations, and extort your money.

- **OUT-OF-THE-BOX COMPLIANCE**

RADICL's advanced threat protection capabilities directly meet and support many compliance requirements.

- **MANAGEABLE SPEED**

We'll offload and accelerate your CMMC journey, aiming to achieve CMMC Level 1 readiness in 90 days and Level 2 in 180 days.

- **COST EFFECTIVE**

We built our platform to deliver enterprise-level cyberprotection and compliance at a reasonable price point. Don't pay more for less.

- **SECURE EVIDENCE CAPTURE**

Evidence from assessments and remediations is securely captured and stored in the our platform. Evidence is centralized, safe, and easily accessible for you and your auditors.

- **EXECUTIVE TRANSPARENCY**

Your CEO and senior leadership will have direct and easy visibility into your compliance posture, ensuring they are in the know and can easily lend a helping hand when needed.

- **AUTOMATIC AND TRUSTWORTHY SPRS SCORE**

Your NIST SP 800-171 SPRS score will be automatically calculated and updated Your NIST SP 800-171 SPRS score will be automatically calculated and updated.

COMPLY WORKFLOW UI

REQUIREMENTS	ASSESSMENT	REMIEDIATION	DOCUMENTS	EXPORTS		
<input type="checkbox"/> SHOW DONE/REJECTED <input checked="" type="checkbox"/> SHOW ACTION REQUIRED <input type="checkbox"/> SHOW READY FOR REVIEW						
Summary	Status	State	Timeframe	Created	Assigned Team	Ultimate Assessor
<input type="checkbox"/> AC.L2-3.1.8 - Unsuccessful Logon Attempts	To Do	Undetermined		03/06/2026 01:36 AM	Compliance Team	London Rojas
<input type="checkbox"/> PE.L1-3.10.3 - Escort Visitors	To Do	Undetermined		03/06/2026 01:36 AM	Compliance Team	London Rojas

RADICL helps simplify, accelerate, and reduce the cost of CMMC compliance.



Visit radicl.com to learn more.