2025 CMMC Level 2 Readiness Guide

Achieve audit-ready compliance with Resilience Cyber Group

This guide helps small and mid-size DoD suppliers understand and prepare for Cybersecurity Maturity Model Certification (CMMC) Level 2, which applies to contractors handling Controlled Unclassified Information (CUI).

Key Requirements & Timeline

- CMMC Level 2 becomes mandatory on November 10, 2025 with a three-year rollout for DoD contracts.
- Contractors must implement the 110 security controls of NIST SP 800-171 and achieve at least an 80% SPRS assessment score.
- Plan of Action & Milestones (POA&M) items must be remediated within 180 days to close gaps.
- Assessments occur every three years: about 37% of the Defense Industrial Base will require Level 2, with 35% needing third-party assessments and only 2% qualifying for self-assessment.
- CMMC is governed by DFARS clauses 252.204-7021 and 252.204-7025; underlying cybersecurity responsibilities remain in effect.

[1] Greenberg Traurig notes Level 2 requires baseline controls, an 80% score and closure of POA&M items within 180 days and that most contractors will need third-party assessments.
[2] DoD CMMC 2.0 guidance states the final rule takes effect on November 10, 2025 with a three-year rollout and alignment with NIST SP 800-171.

Preparing for CMMC Level 2

Success requires a structured approach that aligns your people, processes and technology with the NIST SP 800-171 controls.

- Define the CUI boundary: identify contracts with CUI requirements and map data flows across systems.
- Conduct a NIST 800-171 gap assessment to determine compliance status and risk priorities.
- Develop a System Security Plan (SSP) and POA&M documenting controls and remediation activities.
- Implement technical and policy controls: harden systems, enforce multi-factor authentication, encrypt data in transit and at rest, and train users.
- Remediate POA&M items within 180 days and achieve a minimum 80% SPRS score.
- Perform a self-assessment or engage a certified third-party assessment organization (C3PAO).
- Maintain continuous monitoring and incident response capabilities to ensure evidence of ongoing compliance.

RCG Level 2 Readiness Program

Resilience Cyber Group offers an executive-led readiness program designed to guide contractors through each step of Level 2 compliance. Our deliverables include:

- NIST 800-171 gap assessment and CUI boundary analysis.
- Development of SSP, POA&M, network diagrams and data flow maps.
- Collection of technical evidence and policy artifacts.
- Technical remediation and control implementation guidance.
- Executive advisory sessions and audit preparation.

With a single partner and a clear roadmap, you can achieve Level 2 compliance confidently and efficiently.