CMMC REQUIREMENTS

Cybersecurity Maturity Model Certification (CCMC) 2.0 Overview

LEVEL 1: FOUNDATIONAL

Establishes basic cyber hygiene practices

- Maps to the 15 safeguarding requirements in FAR Clause 52.204-21
- For organizations handling Federal Contract Information (FCI)
- Annual self-assessment required with executive affirmation

LEVEL 2: ADVANCED

Aligned with NIST SP 800-171 (110 controls)

- Applies to organizations handling Controlled Unclassified Information (CUI)
- Compliance path depends on contract criticality:

1. Annual self-assessment, or
2. Triennial third-party assessment (C3PAOs)

- Requires stringent cybersecurity controls

LEVEL 3: EXPERT

Incorporates controls from NIST SP 800-172

- For organizations handling high-priority DoD CUI
- Focuses on defense against Advanced Persistent Threats (APTs)
- Requires triennial DIBCAC assessment
- Highest level of CMMC maturity

Contact Us Today!

1-877-IT-SERVE
learnmore@datalinknetworks.net
www.datalinknetworks.net

datalinknetworks

CORE INSIGHTS

CMMC REQUIREMENTS

Cybersecurity Maturity Model Certification (CCMC) 2.0 Overview

Phase 1 - Initial Rollout (Mid-2025)

- CMMC Level 1& Level 2 self-assessment requirements appear in solicitations
- Level 1: Annual self-assessment + SPRS submission
- Prepare now to remain competitive for DoD contracts

Phase 2 - Level 2 Certification Begins (~Mid-2026)

- Third-party assessments (C3PAOs) become mandatory in solicitations for Level 2

Phase 3 - Level 3 & Option Period Requirements (~Mid-2027)

- DoD introduces Level 3 assessment requirements
- Level 2 certification may become mandatory for existing contract options

Phase 4 - Full Implementation (~Mid-2028)

- All relevant DoD contracts will require applicable CMMC certification
- Applies to all solicitations and option periods, regardless of award date

Stay Ahead of Compliance - Plan Now for CMMC Readiness

Contact Us!

1-877-IT-SERVE
learnmore@datalinknetworks.net
www.datalinknetworks.net

datalinknetworks

CORE INSIGHTS