CMMC 2.0 COMPLIANCE GUIDE

CMMC 2.0 Compliance

Level 1: Foundational

CMMC Level 1 applies to organizations that handle Federal Contract Information (FCI) and focuses on implementing basic cybersecurity safeguards. It requires adherence to 17 practices outlined in FAR 52.204-21, which cover essential areas such as access control, user identification and authentication, media protection, and physical security. Organizations at this level can self-attest to their compliance, meaning no formal third-party assessment is necessary.

- **Scope**: For organizations handling only Federal Contract Information (FCI).
- **Requirements**: Implement 17 basic cybersecurity practices from FAR 52.204-21.
- **Assessment**: Self-attestation is sufficient.
- **Estimated Time**: 1–3 months for preparation and documentation.
- **Estimated Cost**: Minimal if done internally; external consulting may cost $5,000–$15,000.

Level 2: Advanced

CMMC Level 2 applies to organizations that handle Controlled Unclassified Information (CUI) and requires a significantly higher level of cybersecurity maturity. To comply, organizations must implement all 110 security controls outlined in NIST SP 800-171. This includes conducting a readiness assessment to identify gaps, mapping and classifying CUI across systems, and documenting all relevant policies and procedures. Depending on the contract type, organizations must either prepare for a third-party assessment or complete a self-attestation. Continuous compliance is expected, supported by remediation efforts and a maintained Plan of Action and Milestones (POA&M).

- **Scope**: For organizations handling Controlled Unclassified Information (CUI).
- **Requirements**: Implement all 110 controls from NIST SP 800-171.
- **Assessment**: Third-party assessment (C3PAO) required for prioritized acquisitions; self-attestation for others.
- **Estimated Time**:
    - **Preparation**: 3–6 months
    - **Implementation**: 6–12 months
    - **Assessment**: 3–6 months (including scheduling delays)

- **Estimated Cost**:
    - Gap analysis and advisory services: $15,000–$50,000
    - Remediation and implementation: $50,000–$150,000+
    - C3PAO assessment: $20,000–$40,000

Level 3: Expert

CMMC Level 3 is intended for organizations that support critical national security programs and requires the highest level of cybersecurity maturity. Compliance involves implementing advanced security controls from NIST SP 800-172, maintaining strong incident response and threat-hunting capabilities, and demonstrating sophisticated risk management and continuous monitoring practices. Assessments at this level are conducted by government-led teams to ensure rigorous oversight and protection of sensitive information.

- **Scope**: For organizations supporting critical national security programs.
- **Requirements**: Additional controls from NIST SP 800-172, government-led assessments.
- **Estimated Time**: 12–24 months depending on complexity.
- **Estimated Cost**: $250,000+ due to advanced monitoring, incident response, and risk management requirements.

General CMMC Audit Preparation Steps

- Define your CMMC scope.
- Conduct a readiness assessment.
- Classify and map your CUI.
- Implement required security practices.
- Document policies and procedures.
- Remediate gaps.
- Prepare for assessment or self-attestation.
- Leverage technology and tools for automation and monitoring.
- Engage stakeholders in mock interviews.
- Clarify scope with your C3PAO (Certified Third-Party Assessor Organization).
- Be transparent and organized during the audit.

CMMC compliance is no longer optional—it's a critical requirement for organizations working with federal contracts. With enforcement tightening and deadlines approaching fast, now is the time to act. Whether you're handling FCI, CUI, or supporting national security programs, your cybersecurity posture must meet the standards of your assigned CMMC level.

Don't wait until it's too late.

Conduct your readiness assessment, close compliance gaps, and prepare for attestation or formal review.

Call 911 IT today at: **801-997-9444** or visit: **www.911it.com** to get expert guidance, accelerate your compliance process, and ensure your organization is protected and contract-ready.

Your mission, your data, and your future depend on it.