Implementing CMMC Level 2 — With Level 3 Preparedness Built In

How DCAG Helps Prime Contractors Achieve Certification Without Rebuilding Later

For defense contractors, CMMC Level 2 is no longer optional — it is a business continuity requirement. But many organizations approach Level 2 as a checklist exercise, only to discover later that their architecture cannot scale to Level 3 or withstand DIBCAC scrutiny.

At Data Center Assistance Group (DCAG), we guide organizations to implement CMMC Level 2 correctly the first time — with structural readiness for Level 3 maturity.

The Problem: Compliance Without Architecture

Most CMMC initiatives fail for predictable reasons:

- Undefined enclave boundaries
- CUI sprawl across enterprise systems
- Weak Organization-Defined Parameters (ODPs)
- SSPs that do not match operational reality
- Insufficient evidence for live assessor validation
- Supply chain oversight gaps
- No continuous monitoring model

These failures are rarely technical. They are governance failures.

The DCAG Approach: Architecture + Governance + Evidence

DCAG implements CMMC as an executive-controlled program — not an IT project.

1. Enclave Strategy Design

We help clients establish a clearly defined CUI Security Enclave aligned with NIST SP 800-171 Rev. 3 scoping principles.

This limits compliance exposure and creates a hardened, monitored environment dedicated to protecting CUI.

Think of it as building a vault inside the enterprise — instead of turning the entire building into a vault.

2. Executive Program Authority

We develop formal Program Authority Statements and governance frameworks that:

- Define accountability
- Assign risk ownership
- Establish scope control rules
- Formalize ODP decisions
- Prepare executives for certification affirmation

This protects leadership and strengthens fiduciary posture.

3. Control Implementation & Evidence Engineering

DCAG maps all 110 Level 2 security requirements to:

- Operational controls
- Assessment objectives
- Evidence artifacts
- Live demonstration readiness

We engineer systems so that evidence is continuously generated — not assembled weeks before an audit.

4. DIBCAC-Ready Mock Assessments

Prime contractors must assume High Assessment scrutiny.

We simulate:

- Live configuration validation
- Account lifecycle traceability
- Log integrity testing
- Boundary enforcement review
- Supply chain documentation analysis

This eliminates surprises during C3PAO or DIBCAC engagement.

Level 3 Preparedness — Built Into the Foundation

Many organizations implement Level 2 controls in a way that requires redesign to reach Level 3.

DCAG builds enclave architectures that are:

- Zero Trust–ready
- Logging scalable
- Threat-informed
- Segmentation hardened
- Supply chain defensible
- Continuous monitoring capable

This ensures Level 3 becomes an incremental maturity step — not a reconstruction effort.

Continuous Monitoring and Board Reporting

Compliance is not static.

We help organizations implement:

- Real-time compliance dashboards
- Drift detection
- POA&M governance tracking
- Risk trend analysis
- Executive reporting models

This supports Board due diligence and reduces certification renewal risk.

Why It Matters

CMMC is not simply a cybersecurity framework. It is:

- A contract eligibility requirement
- A reputational safeguard
- A supply chain trust signal
- A fiduciary responsibility

Organizations that approach it strategically strengthen their competitive position.

Organizations that approach it tactically risk costly remediation and contract disruption.

DCAG's Value

DCAG brings:

- Executive-level governance alignment
- Enterprise resilience expertise
- Prime contractor experience

- Architecture-driven compliance design
- Scalable enclave implementation models
- Level 2 to Level 3 transition planning

We do not implement compliance theater.
We build defensible security operating models.

Call to Action

Thomas Bronack, President

Data Center Assistance Group, LLC

bronackt@gmail.com | (917) 673-6992