CMMC Level 2 Certification Strategy
Executive Interview Briefing

Prepared for Leadership Team

Thomas Bronack, CBCP
President, DCAG

Program Objective

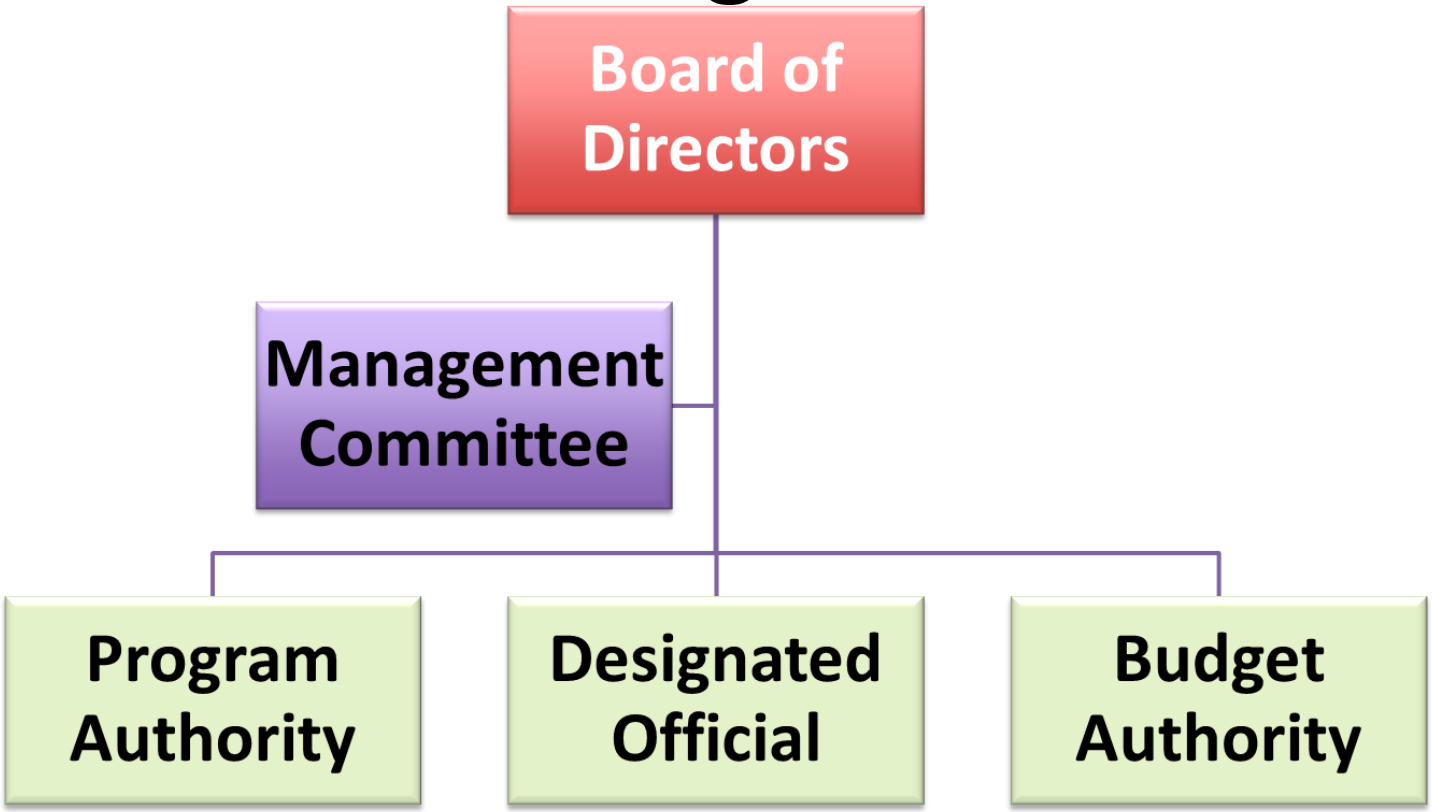
- Achieve CMMC Level 2 Certification
  - Protect CUI across global operations
  - Establish sustainable governance model
  - Enable continued DoD contract eligibility

- **CMMC protects Controlled Unclassified Information (CUI) and Federal Controlled Information (FCI) within the DoD Supply Chain.**

Governance Model

- Getting the Team together
- Executive Sponsor + Steering Committee
  - Dedicated CMMC Program Office
  - Cross-Functional IS/IT Workstreams
  - Monthly Financial & Risk Reporting
  - Awareness and CMMC team Training

CMMC Management Chart



- Who owns the CMMC program?
- Who signs the certification affirmation?
- Who accepts residual risk?

- CMMC designated to determine if compliance requirements are et.
- This role must be assigned.

- Multi-year funding approval
- Tooling authority
- Staffing approval
- MSP/MSSP contractual authority

The Roles played by ISO 27001, ISO 27701, and NIST SP 800-171

Think of ISO 27001 as the executive management and governance operating system for cybersecurity.

ISO/IEC 27701 extends ISO 27001 into privacy governance and personally identifiable information (PII) protection.

ISO 27701 essentially overlays a privacy compliance and regulatory accountability layer onto ISO 27001

NIST 800-171 is operationally deeper and more technical than ISO 27001.

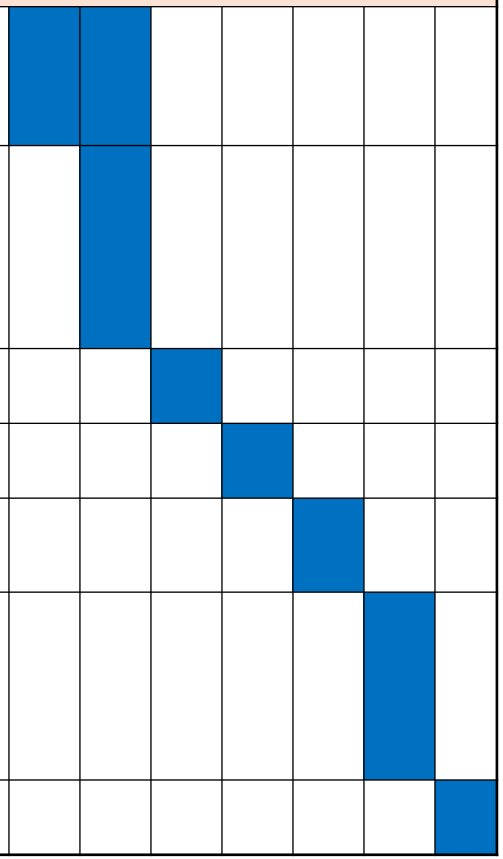
How they Integrate Operationally

Framework	Primary Focus	Role in Governance Stack
ISO 27001	Enterprise security governance	Defines the security management system
ISO 27701	Privacy governance	Extends ISMS into privacy and PII protection
NIST SP 800-171	Technical security controls	Enforces operational safeguards for sensitive data (CMMC)

Together they demonstrate:

- Due diligence
- Due care
- Operational maturity
- Governance transparency
- Regulatory readiness
- Supply-chain trustworthiness

CMMC Level 2 Certification Program Timeline

CMMC Level 2 Certification Program Timeline	
Phase 1: Program initiation, Governance & CUI Boundary Definition (ISO 27001 / ISO 27701).	
Phase 2: NIST 800-171 Gap Assessment & System Security Plan (SSP) Development	
Phase 3: Control Remediation & Technical Implementation	
Phase 4: Evidence Repository Consolidation & Validation	
Phase 5: Mock C3PAO Pre-Assessment Simulation	
Phase 6: Potential DIBCAC Voluntary Assessment for SPRS Score and Gap Analysis.	
Phase 7: Formal C3PAO Certification Assessment	

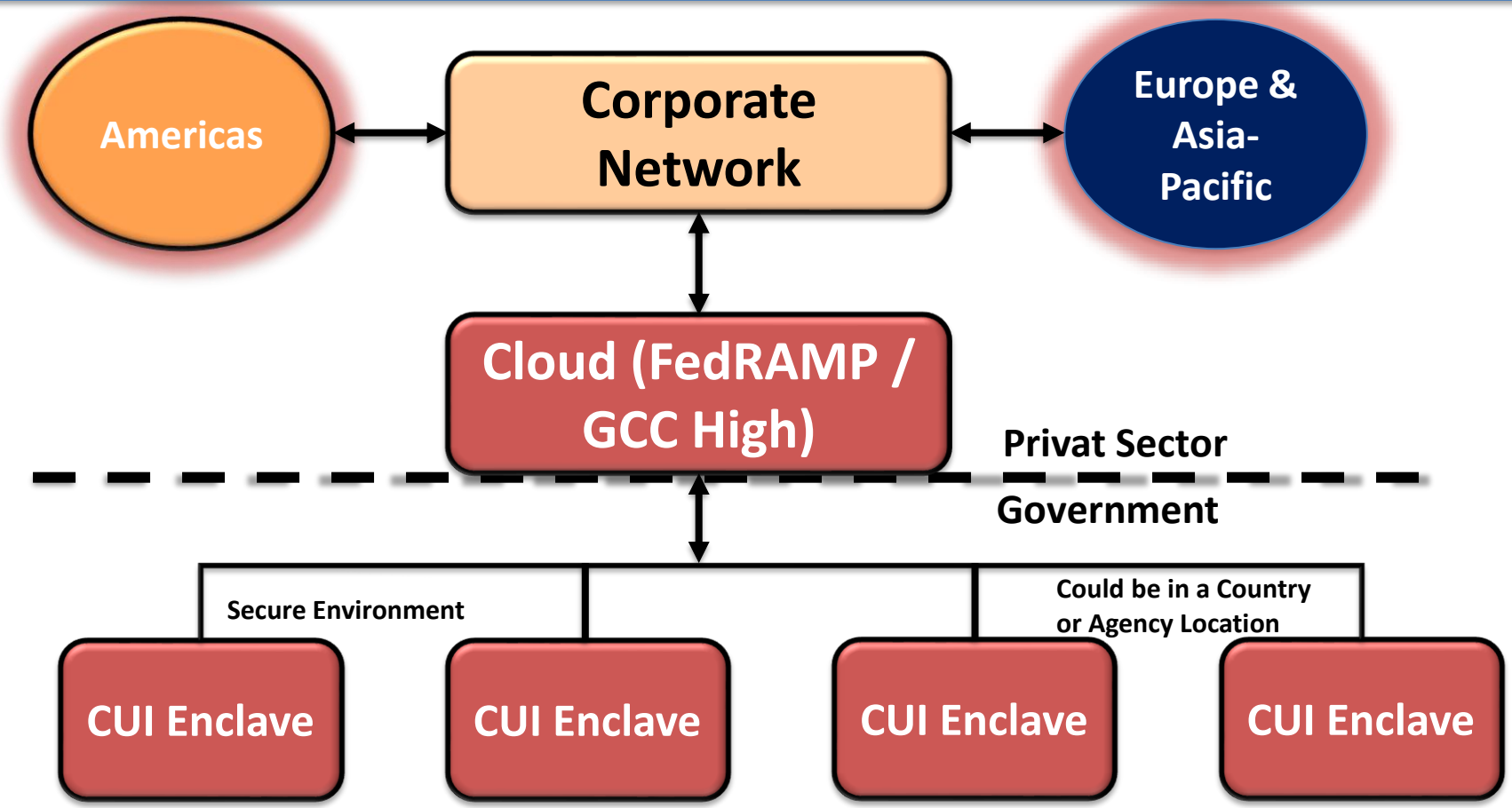
The seven essential Security Documents every company needs

1. Information security Policy (ISP).
2. Incident Response Plan (IRP)/
3. Business Continuity & Disaster Recovery (BCP/DR).
4. Access Control and Identity Management AC/IM).
5. Vendor and Third-Party Risk Management (TPRM).
6. Security Awareness & Acceptable Use.
7. AI Governance & Model Risk Management.

Security Preparedness Process

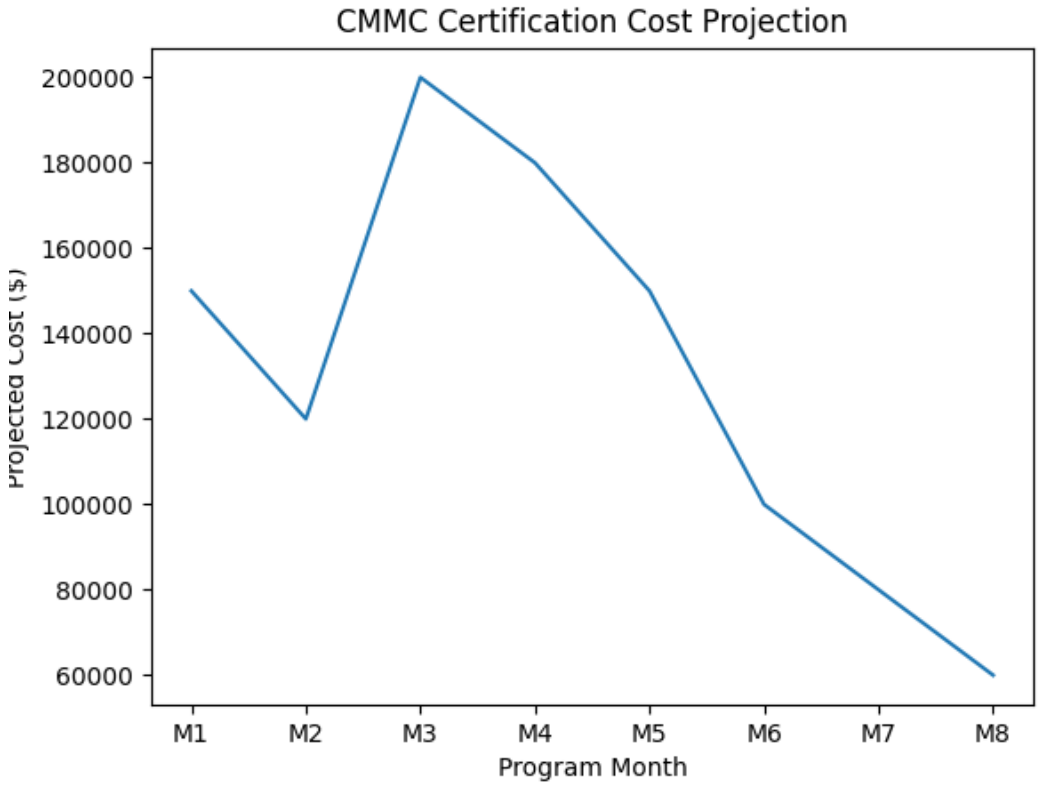
1. Define Objectives
2. Perform a Risk Assessment
3. Formalize Security & Procedures
4. Physical and Data Security
5. Personal Security
6. Technical / Electrical Security
7. Operational Security
8. Incident Response & Emergency Plans
9. Information Security
10. Training & Awareness
11. Monitoring & Reporting.

CUI Boundary Architecture Model



A CUI enclave is a secure, isolated IT environment designed to protect Controlled Unclassified Information (CUI) while simplifying compliance with federal cybersecurity standards.

Financial Model – Cost Projection



Top Program Risks

- CUI Scope Misdefinition
  - Incomplete Evidence Repository
  - Cross-Border Data Conflicts
  - Tool Integration Gaps
  - Schedule Compression Risk
  - Documentation & Runbooks
  - Awareness & Training

90-Day Execution Focus

- Days 1–30: Scope & Control Heatmap
  - **Days 31–60:** Launch Remediation Sprints
  - **Days 61–90:** Evidence Consolidation & Mock Review
  - Establish Audit-Ready Culture
  - Embedded in everyday functions and automated when possible

Other Services DCAG Provides

Contact:

Thomas Bronack, President
Data Center Assistance Group, LLC
bronackt@dcag.com |
bronackt@gmail.com
https://www.dcag.com
(917) 673-6992

- **Executive and Board Level due diligence and fiduciary management support.**
- **Application Factory with adjustable quality control gates and automation to achieve Authorization to Operate (ATO).**
- **Continuous Threat Exploitation Management (CTEM) to achieve continuous ATO (cATO).**
- **Vulnerability Management with Patch and Release Management.**
- **Vendor and Third-Party Risk Management.**
- **Supply Chain Management, with Contracts and SLAs.**
- **Risk and Security Management, with CMMC.**
- **Quantum Readiness and Pos-Quantum Cryptography (PQC)**
- **Program/Project and Team Management.**
- **Documentation, Awareness, and Training services.**
- **Technical and Managerial services.**