CSF 2.0 Cybersecurity Readiness

Operationalizing Cyber Resilience Across Your Enterprise

1. Executive Summary

The NIST Cybersecurity Framework 2.0 (CSF 2.0) offers a powerful structure for improving an organization's cybersecurity posture while aligning with business objectives and regulatory mandates. At Data Center Assistance Group, LLC (DCAG), we help enterprises assess, implement, and operationalize CSF 2.0 across all six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Our consulting services offer both strategic vision and operational execution—bridging executive oversight and frontline security operations through customized readiness plans, scorecards, and remediation guidance.

2. Business Challenge

Organizations often struggle with:

- Fragmented cybersecurity programs and unclear priorities
- Incomplete alignment between governance, risk, compliance (GRC), and technical operations
- Lack of formalized cybersecurity governance practices
- Difficulty operationalizing framework controls in real environments
- Inability to measure and report cybersecurity maturity effectively

3. Our Solution

DCAG offers CSF 2.0 Cybersecurity Readiness Services tailored to your maturity level, industry, and regulatory context. We guide stakeholders in using CSF 2.0 as both a planning and operational tool. Whether you are adopting the framework for the first time or seeking to improve existing implementation, our services provide a roadmap to measurable resilience.

Services include:

- CSF 2.0 Readiness Assessments and Maturity Scoring
- Control Mapping across frameworks (NIST 800-53, ISO 27001, CMMC)
- Executive and Board Reporting Dashboards
- Playbooks for each CSF Function, with clear ownership and KPIs
- Guidance for integrating CTEM, DevSecOps, and threat modeling into CSF functions

4. Key Service Components

- ✅ Full Lifecycle Coverage of CSF 2.0 (Govern, Identify, Protect, Detect, Respond, Recover)

- ✅ Readiness Assessments and Maturity Scoring
- ✅ Control Gap Analysis and Action Planning
- ✅ Executive Dashboards and Scorecards
- ✅ Framework Integration (NIST, ISO, CMMC, EO 14028, OMB, SEC 2023-139)
- ✅ Functional Playbooks with Control Ownership
- ✅ Risk-to-Readiness Alignment Workshops
- ✅ Incident Simulation and Response Integration

5. Outcomes & Business Value

Engaging DCAG for CSF 2.0 Cybersecurity Readiness enables:

- Improved Maturity & Measurable Progress
- Stronger Cyber Resilience
- Executive Buy-In
- Cross-Framework Compliance
- Informed Investment Planning

6. Engagement Approach

We offer tailored engagement levels to match your starting point and compliance trajectory:

Engagement Level	Description	Best For
Foundational Assessment	Baseline review of CSF 2.0 posture and maturity scoring	First-time adopters or annual reviews
Remediation Roadmap	Detailed POA&M and control alignment with implementation guides	Organizations needing alignment or improvement
CSF Integration Services	Embed CSF into DevSecOps, IR, and governance processes	Enterprise IT and cybersecurity teams
CSF PMO Oversight	Ongoing CSF governance, board briefings, and updates	Regulated or high-risk organizations

7. Ready to Operationalize CSF 2.0?

CSF 2.0 is not just a framework—it's a roadmap to resilience. DCAG is ready to support your leadership, security teams, and compliance stakeholders in making cybersecurity maturity measurable, achievable, and aligned with your business goals.

Contact:
Thomas Bronack, CBCP
Founder & Executive Consultant
📧 bronackt@gmail.com | 📞 (917) 673-6992
Data Center Assistance Group, LLC