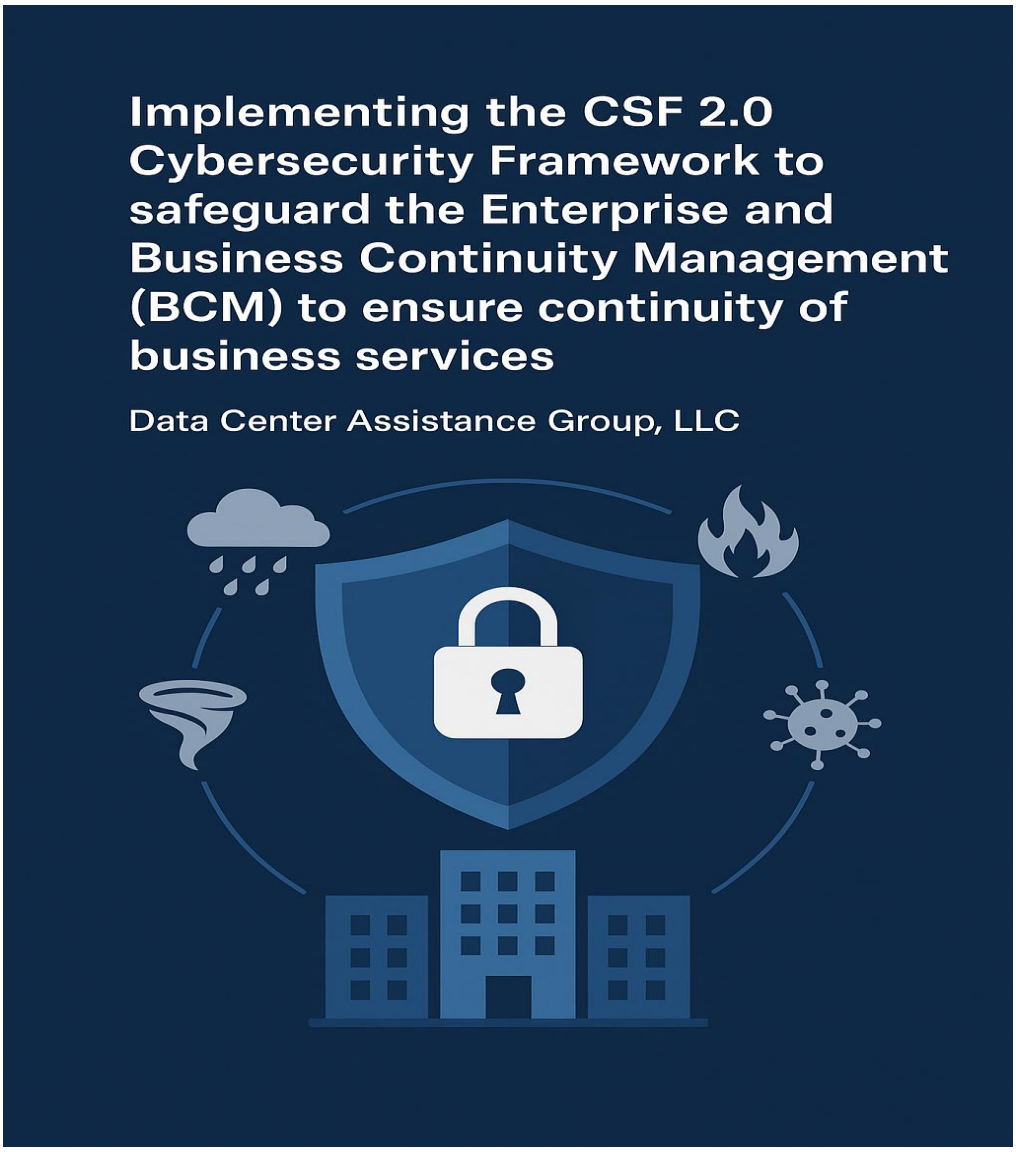
Protecting Healthcare and other Enterprises against cybercrimes and providing continuity of business



By Thomas Bronack, President
Data Center Assistance Group, LLC
Email: bronackt@dcag.com or bronackt@gmail.com
Phone: 917-673-6992
Website: https://www.dcag.com

Executive Briefing: Aligning Business Continuity with Cybersecurity through NIST CSF 2.0

Prepared for: Executive Leadership Team | Date: July 2025

Prepared by: Enterprise Resilience Advisor

Overview

In today's threat landscape, healthcare organizations face unprecedented pressure from cyberattacks, regulatory scrutiny, and operational disruptions. With ransomware, third-party data breaches, and quantum-era threats on the rise, it is no longer sufficient to treat Business Continuity (BC) and Cybersecurity as isolated functions.

NIST Cybersecurity Framework (CSF) 2.0 provides a unified model that integrates cybersecurity risk with organizational resilience. Aligning BC and cybersecurity under this framework ensures healthcare delivery, patient data protection, and regulatory compliance—especially as digital transformation accelerates.

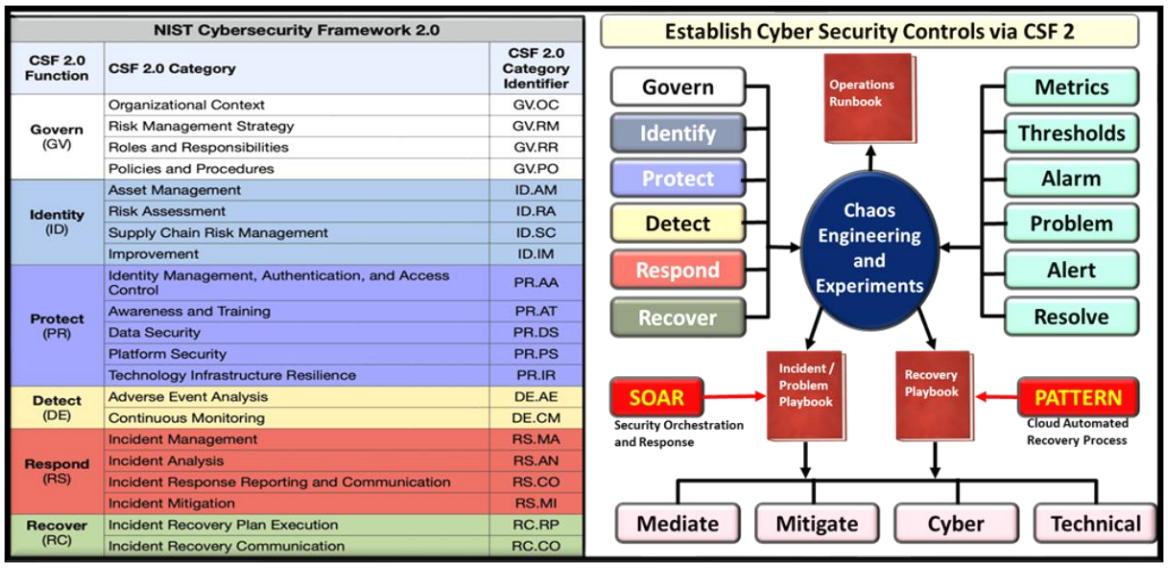
Why This Alignment Matters in 2025

- Cyber incidents now disrupt care delivery and enterprise functions—not just IT systems.
- HIPAA, HITECH, and ONC Cures Act require proactive, integrated risk management.
- Patient trust is business currency. A single ransomware attack can cost millions and damage reputation irreparably.
- Resilience is now a C-Suite responsibility, not just a compliance checkbox.

Risk-to-Business Impact Chart

Risk Scenario	Business Impact if Unaligned	Mitigation with BC + Cyber Alignment
Ransomware attack on EHR system	Patient care halted, compliance violations, data breach fines	Integrated response and recovery protocols reduce downtime
Supply chain software compromise	Exposure to third-party vulnerabilities, regulatory fallout	Continuous SBOM review tied to BC incident planning
Power or IT outage in ICU or lab	Critical care disruption, legal exposure, patient safety risks	Cyber-informed BC planning enables prioritized recovery
Unpatched medical IoT device exploited	Lateral breach into clinical systems, compromised diagnostics	Joint vulnerability tracking and system recovery drills
Insider misconfiguration during incident response	Extended outage, amplified threat exposure	Cyber and BC teams coordinate roles during escalations

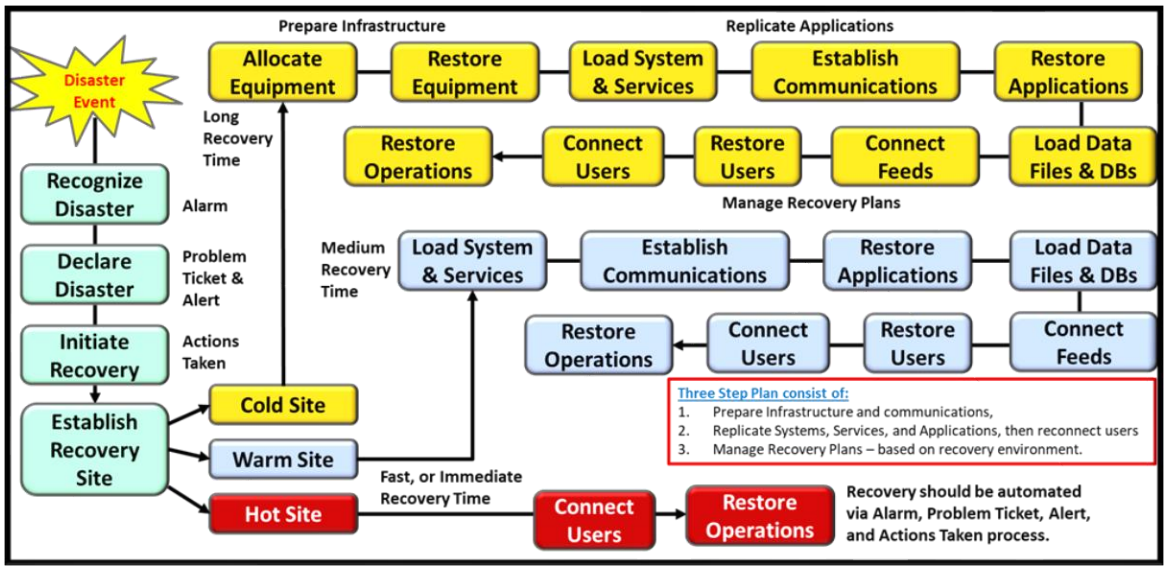
CFS 2.0 Description and integration



NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

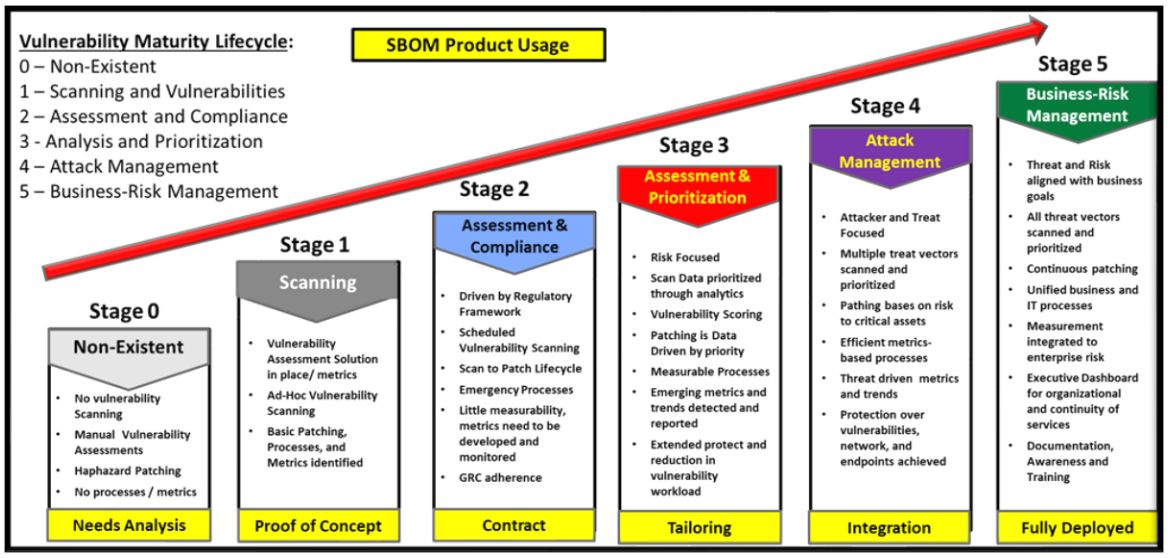
[Cybersecurity Framework 2.0 / NIST explanation.]

Business and Disaster Recovery concepts



Types of recovery that should be integrated within your environment.

Vulnerability Management Life Cycle



Vulnerability Management is an FDA requirement and provides a means to ensure all components are at current release levels and free of KNOWN vulnerabilities.

Next-Step Recommendation

We recommend that the executive team initiate an enterprise-wide Resilience Integration Project guided by NIST CSF 2.0. This includes:

1. Governance Alignment: Establish shared oversight of cybersecurity and business continuity under one strategic resilience committee.
2. Integrated Risk Assessments: Combine IT threat modeling and BC impact analyses for more realistic prioritization.
3. Cyber-Resilient Playbooks: Develop joint response playbooks for top risk scenarios with cross-functional rehearsals.
4. Continuous Monitoring: Leverage shared dashboards for threat, compliance, and continuity metrics.
5. Quarterly Board Reporting: Present unified risk-resilience posture to drive investments and accountability.

Final Thought

Aligning BC and cybersecurity is no longer optional—it is a strategic imperative. Using NIST CSF 2.0 as a blueprint provides healthcare organizations with a tested, adaptive structure to protect lives, sustain trust, and preserve mission-critical operations.

CERT – Resilience Maturity Model (RMM)

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training & Awareness
RISK	Risk Management

Operations Management	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies
ID	Identity Management
IMC	Incident Management & Control
KIM	Knowledge & Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis & Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

4 Categories with 26 Process Areas

1. Enterprise Management
2. Operations Management
3. Process Management
4. Engineering

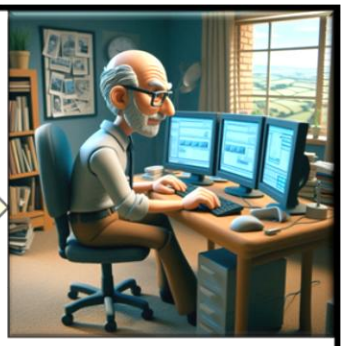
CERT-RMM is a **maturity model** that promotes the convergence of security, business continuity, and IT operations activities to help organizations actively direct, control, and manage operational resilience and risk.

Call to Action

- **Discuss**
- **Define**
- **Propose**
- **Achieve**

Quality Service at a Reasonable Price

Helping Clients to achieve success



If you find the information included in this presentation of value and want to explore methods to improve the reliability of your enterprise and IT environment, please contact me to discuss your needs and request our assistance.

We look forward to our future relationship.

Thomas Bronack, CBCP
President
Data Center Assistance Group, LLC
Website: http://www.dcag.com
bronackt@dcag.com
bronackt@gmail.com
917-673-6992

