Enterprise Resilience and Governance

Enterprise Resilience - 30-60-90 Day Evaluation of Execution Plan

Prepared for Executive Leadership

Created By:

Thomas Bronack, President

Data Center Assistance Group, LLC

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

Table of Contents

Contents

Executive Positioning Statement 3
Executive Analogy: Building a Resilient City 3
Key Performance Indicators (KPIs) 4
30-60-90 Execution Summary 4
30 Days: Functions Performed 5
60 Days: Functions Performed 6
90 Days: Functions Performed 7
Executive Dashboard 8
Performance Trends 8
System Performance Coverage score, can include: 8
Governance Model 9
Business Continuity Management 10
Business Continuity Management includes: 10
Governance, Risk, and Compliance Laws and Regulations 11
Domestic and International Laws and Regulations impacting ERG. 11
Domestic (USA) 11
International 14
NIST Frameworks you should be familiar with 16
Executive readout 17
Call to Action 17

Executive Positioning Statement

What this paper provides is the ability to move from Enterprise Resilience and Governance (ERG) planning to a proven recovery certification capability. It is focused on ensuring that when disruption happens -and it will - the organization knows exactly what to do, how long recovery will take, and how to execute with confidence.

This paper establishes a structured evaluation and execution roadmap across a 30-60-90-day horizon, designed to clearly define the organization's current Enterprise Resilience Governance (ERG), Business Continuity Management (BCM), and Crisis Management maturity. It provides leadership with a validated baseline from which to build a disciplined, end-to-end recovery capability—ensuring that critical business services remain uninterrupted, recovery objectives are measurable and achievable, and organizational responsibilities are met with confidence and compliance.

Executive Analogy: Building a Resilient City

- **30 Days:** Survey the land and identify risks.
- **60 Days:** Build infrastructure and validate operations.
- **90 Days:** Optimize and scale into a resilient ecosystem.

 © Data Center Assistance Group, LLC

Key Performance Indicators (KPIs)

Metric	Definition	Target	Executive Value
RTO Achievement	Recovery time vs objective	>95%	Predictable recovery
DR Test Success Rate	Successful recovery tests	>90%	Validated capability
Critical Coverage	Systems with DR plans	100%	Reduced exposure
Risk Exposure	Open resilience risks	<5%	Controlled risk posture
RTC Measurement	Recovery Time Capability measured and quantitated	<10-15%	Reduce the time and effort required to detect, and initiate recovery operations

30-60-90 Execution Summary

Phase	Focus	Key Activities	Deliverables	Outcome
30 Days	Assess	BIA, risk analysis, stakeholder alignment	Maturity assessment, risk list	Visibility
60 Days	Execute	DR testing, playbooks, dashboards	Evaluate results, remediation tracker	Validated recovery
90 Days	Scale	Optimization, audit prep, training	Audit-ready package	Enterprise resilience

 © Data Center Assistance Group, LLC

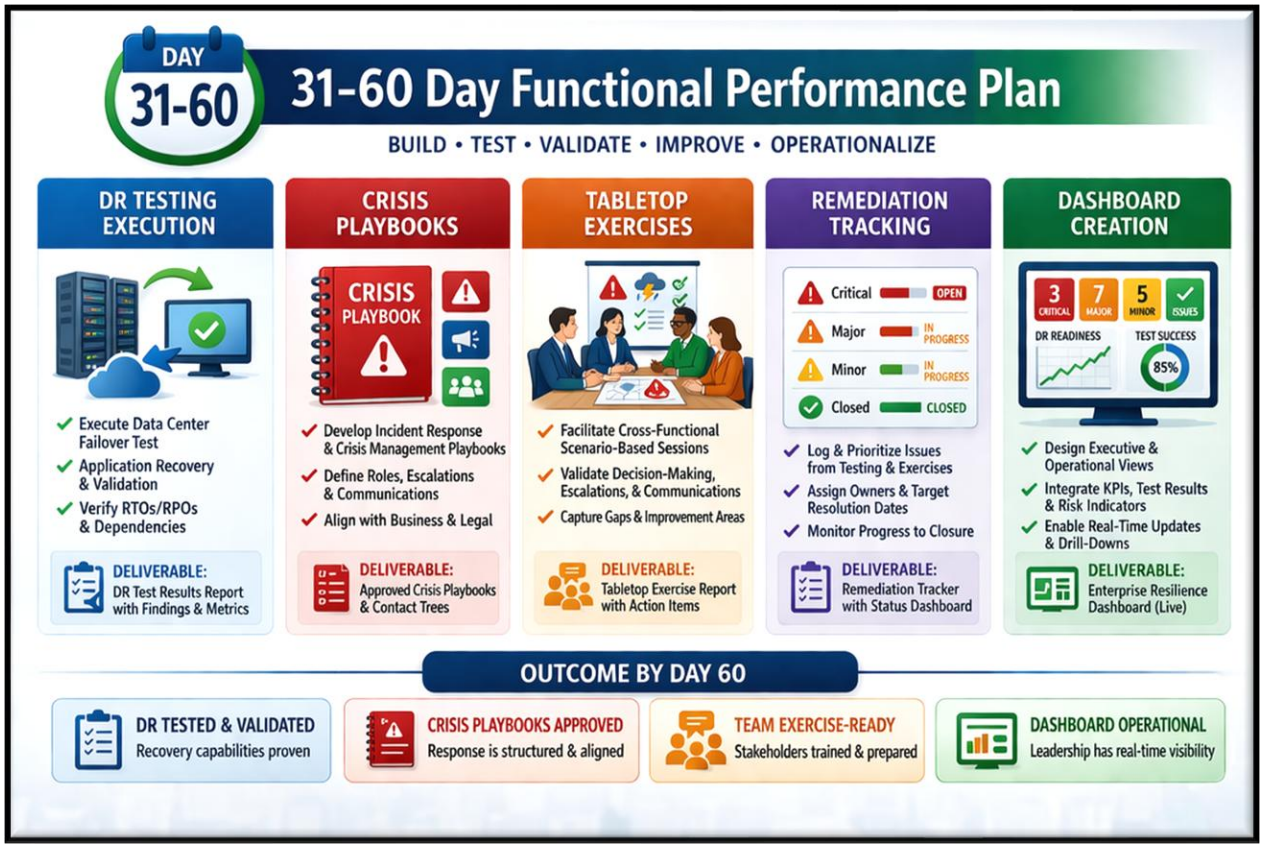
30 Days: Functions Performed

- Program assessment
- BIA validation
- Risk identification
- Stakeholder alignment
- Governance setup

 © Data Center Assistance Group, LLC

60 Days: Functions Performed

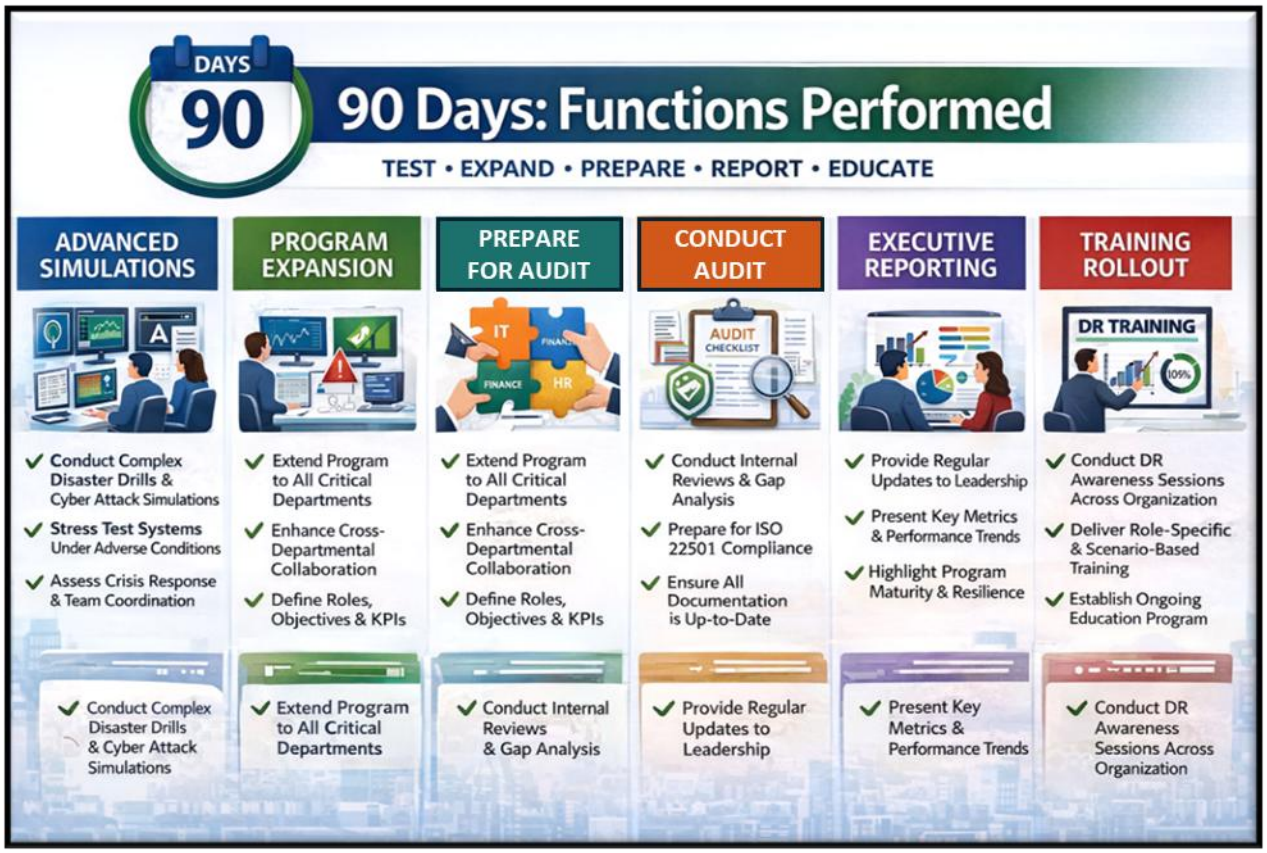
- DR testing execution
- Crisis playbooks
- Tabletop exercises
- Remediation tracking
- Dashboard creation



 © Data Center Assistance Group, LLC

90 Days: Functions Performed

- Advanced simulations
- Program expansion
- Audit readiness
- Executive reporting
- Training rollout



 © Data Center Assistance Group, LLC

Executive Dashboard

- RTO Performance Trend
- - DR Test Success Rate
- - Risk Heat Map
- - System Coverage

Performance Trends

- Upward trending represents reduced RTO and improved efficiency at reduced costs with less stain on clients and staff resulting in greater customer satisfaction and reputation.
- As DR Test Rate approaches 100%, it indicates your organization's ability to provide continued business Product/Service continuity throughout a range of interruptions.
- As the Heat Map becomes Greener, your organization improves reliability.

System Performance Coverage score, can include:

- 100% of products/Services requiring ERG Certification identified.
- 85% of Identified Products/Services being ERG Certified are Rated (1-5).
- 72% of Rated Products/Services are being ERG certified.
- 42% of Products/Services are not yet scheduled, or failed, certification.

 © Data Center Assistance Group, LLC

Governance Model

- Strategic Layer: Executive decisions and risk acceptance
- Operational Layer: Program management and reporting
- Execution Layer: Engineering and IT recovery implementation

 © Data Center Assistance Group, LLC

Business Continuity Management

Business Continuity Management includes:

1. Business Recovery should a business office or location suffer a disaster event.
2. Disaster Recovery when the data center experiences hardware, software, or networking failure.
3. Emergency Management should a natural disaster occur.
4. Crisis Management to prepare for responses to event types.
5. Supply Chain deliveries should be resolved if an office is moved to a remote location.
6. First Responders will take over the site when an emergency occurs. After they leave, your company security should provide site protection to prevent looting or the theft of critical data.
7. Salvage and Restoration services must be commissioned to clean damaged site, salvage any materials and equipment not damaged beyond use, and restore the location to post disaster event operation.
8. Management will evaluate if site is ready to be reoccupied and personnel will gradually return after restoration.
9. Preparations for personnel to work at home or other locations must be made.
10. Site Recovery and Data Center Recovery locations must be contracted.

 © Data Center Assistance Group, LLC

Governance, Risk, and Compliance Laws and Regulations

Domestic and International Laws and Regulations impacting ERG.

Domestic (USA)

Sector	Law / Regulation	Purpose	Issued by	Description	Penalty
Banking	**FFIEC Business Continuity Management Booklet**	Ensure availability of critical financial services	FFIEC	Examiner guidance for BCM governance, BIA, interdependency analysis, resilience strategies, crisis management, testing, maintenance, and board reporting for financial institutions.	**Medium**
Banking / Financial	**Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, 16 CFR Part 314**	Protect customer information	FTC	Requires covered financial institutions to develop, implement, and maintain safeguards for customer	**High**

Sector	Law / Regulation	Purpose	Issued by	Description	Penalty
				information and oversee service providers; now also includes certain security-event reporting.	
Securities / Financial Markets	**SEC Regulation SCI**	Preserve systems compliance, integrity, and operational resilience of key market systems	SEC	Applies to certain market entities and requires controls for SCI systems, including handling systems disruptions and compliance issues affecting regulated activities.	**High**
Banking / Financial / Insurance (New York)	**23 NYCRR Part 500**	Cybersecurity governance and protection of nonpublic information	New York State Department of Financial Services	Requires a cybersecurity program, governance, vulnerability management, audit trail, access controls, risk assessment, training, and incident-related measures for covered entities.	**High**
Hospital / Healthcare	**HIPAA Security Rule**	Protect confidentiality, integrity, and availability of ePHI	HHS OCR	Establishes administrative, physical, and technical safeguards for ePHI; the contingency plan standard includes backup, disaster recovery, emergency mode operations, testing, and criticality analysis.	**High**
Hospital / Healthcare	**CMS Emergency Preparedness Rule**	Ensure provider readiness for natural and man-made disasters	CMS	Requires Medicare/Medicaid participating providers and suppliers to maintain emergency plans, communication plans, policies/procedures,	**High**

Sector	Law / Regulation	Purpose	Issued by	Description	Penalty
				testing, and compliance as a condition of participation.	
Pharmaceutical	**Current Good Manufacturing Practice (CGMP), 21 CFR Parts 210/211**	Assure product quality, strength, identity, and purity	FDA	Requires controls over methods, facilities, and manufacturing/packing operations for drugs; operational discipline and documented controls are core resilience enablers for pharma operations.	**High**
Government	**FISMA (Federal Information Security Modernization Act)**	Establish federal information security program requirements	U.S. Congress / OMB / DHS / NIST implementation ecosystem	Requires federal agencies to develop, document, and implement agency-wide information security programs and undergo annual reporting/assessment.	**High**
Manufacturing / Pharma / Chemicals	**OSHA Process Safety Management (29 CFR 1910.119)**	Prevent or minimize catastrophic releases of highly hazardous chemicals	OSHA	Requires employers handling threshold quantities of hazardous chemicals to implement integrated management practices, procedures, and controls to prevent major incidents.	**High**
Manufacturing / Chemicals	**EPA Risk Management Program Rule (40 CFR Part 68)**	Chemical accident prevention and emergency preparedness	EPA	Requires facilities using certain hazardous substances to develop a Risk Management Plan and implement accident-prevention and emergency-preparedness measures.	**High**

International

Sector	Law / Regulation	Purpose	Issued by	Description	Penalty
Banking / Financial (EU)	**DORA — Regulation (EU) 2022/2554**	Strengthen digital operational resilience in financial services	European Union	Creates a dedicated EU framework for digital operational resilience in the financial sector, covering ICT risk, resilience testing, incident handling/reporting, and third-party risk. It has been applied since **January 17, 2025**.	**High**
Banking / Financial (UK)	**FCA / PRA Operational Resilience Rules**	Keep important business services within impact tolerances during severe disruptions	FCA / PRA / Bank of England	Requires firms to identify important business services, set impact tolerances, map dependencies, test vulnerabilities, remediate, and maintain communication plans; firms were expected to complete mapping/testing by **March 31, 2025**.	**High**
Cross-sector critical services (EU)	**NIS2 Directive — Directive (EU) 2022/2555**	Establish a common cybersecurity baseline across critical sectors	European Union	Creates a unified legal framework across **18 critical sectors** and applies to sectors including banking, healthcare, manufacturing, and public administration/critical entities depending on national implementation.	**High**
Cross-sector	**GDPR — Regulation (EU) 2016/679**	Protect personal data and regulate processing	European Union	Applies broadly across sectors processing EU personal data; resilience relevance is strongest around	**High**

Sector	Law / Regulation	Purpose	Issued by	Description	Penalty
				availability, integrity, breach handling, governance, and operational controls protecting personal data.	
Hospital / Medical Device / Pharma Supply Chain (EU)	**Medical Device Regulation (MDR) — Regulation (EU) 2017/745**	Ensure safety, performance, traceability, and lifecycle control of medical devices	European Union	Strengthens lifecycle governance, testing, conformity assessment, and traceability for medical devices, supporting resilience in device manufacturing and hospital supply chains.	**High**
Manufacturing / Software / Connected Products (EU)	**Cyber Resilience Act (CRA) — Regulation (EU) 2024/2847**	Impose cybersecurity requirements on products with digital elements	European Union	Sets horizontal cybersecurity requirements for software and hardware products with digital elements, addressing insecure products and weak patch/update practices.	**High**
Financial / Healthcare / Data Processing / Critical Infrastructure (Australia)	**Security of Critical Infrastructure Act 2018 (SOCI Act)**	Protect critical infrastructure and set security/resilience obligations	Australian Government	Applies across sectors including **financial services and markets**, **data storage or processing**, and **healthcare and medical**, and establishes legal obligations for owners/operators of critical infrastructure assets.	**High**
Banking / Financial / Pharma / Manufacturing / Healthcare	**PIPEDA**	Regulate private-sector handling of personal information in	Parliament of Canada / OPC oversight	Canada's federal private-sector privacy law; applies to organizations collecting, using, or	**Medium**

Sector	Law / Regulation	Purpose	Issued by	Description	Penalty
(Canada private sector)		commercial activity		disclosing personal information in commercial activity, with direct governance and resilience implications for data handling and breach response.	

NIST Frameworks you should be familiar with

Framework:	Description:
NIST Cybersecurity Framework (CSF 2.)	Provides cybersecurity risk management guidance for industry, government agencies, and other organizations to help them understand, assess, prioritize, and communicate their cybersecurity efforts.
NIST SP 800-53	Provides a catalog of security and privacy controls for information systems and organizations. It forms the foundation for building a strong control environment and is frequently referenced in compliance audits.
NIST Risk Management Framework (RMF) — SP 800-37	Provides a structured process for managing risk to information systems, from categorization to continuous monitoring. It helps to ensure that risks are identified, documented, and accepted in information systems.
NIST SP 800-171	Provides recommended security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems and organizations. If you work with government contracts or defense contractors, this is the one you'll see often.
NIST SP 800-30	Provides guidance for conducting risk assessments. It provides a step-by-step process for identifying threats, vulnerabilities, and risks to systems.
NIST SP 800-61	Provides guidance on how to incorporate cybersecurity incident response in risk management activities. This can help organizations prepare for, detect, and respond to cybersecurity incidents while minimizing their impact.
NIST SP 800-122	Provides guidance on how to protect the confidentiality of personally identifiable information (PII) in information systems. It helps organizations identify PII and determine the appropriate level of protection for each instance.

 © Data Center Assistance Group, LLC

Executive readout

The highest-impact regulatory instruments for **resilience program design** are usually:

- **Banking / financial:** FFIEC BCM, GLBA Safeguards Rule, SEC Reg SCI, NYDFS Part 500, DORA, UK operational resilience.
- **Healthcare / hospitals:** HIPAA Security Rule, HITECT Act, CMS Emergency Preparedness Rule, MDR where device operations are in scope.
- **Pharma / manufacturing:** FDA CGMP, OSHA PSM, EPA RMP, CRA for digital products, and NIS2 where EU critical-sector coverage applies.
- **Government:** FISMA remains the anchor U.S. federal governance statute for information security programs.

A devil's-advocate caution: **"enterprise resilience" is not governed by one universal law.** In practice, organizations are regulated through a **patchwork** of sector rules covering **security, continuity, emergency preparedness, safety, data protection, market integrity, and product assurance**. Governance failures usually happens when firms treat these as separate compliance silos instead of one integrated resilience program.

Call to Action

If you would like a 90-day evaluation of your existing Enterprise Resilience and Governance functions as described in this document, contact Thomas Bronack at:

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