
Created by

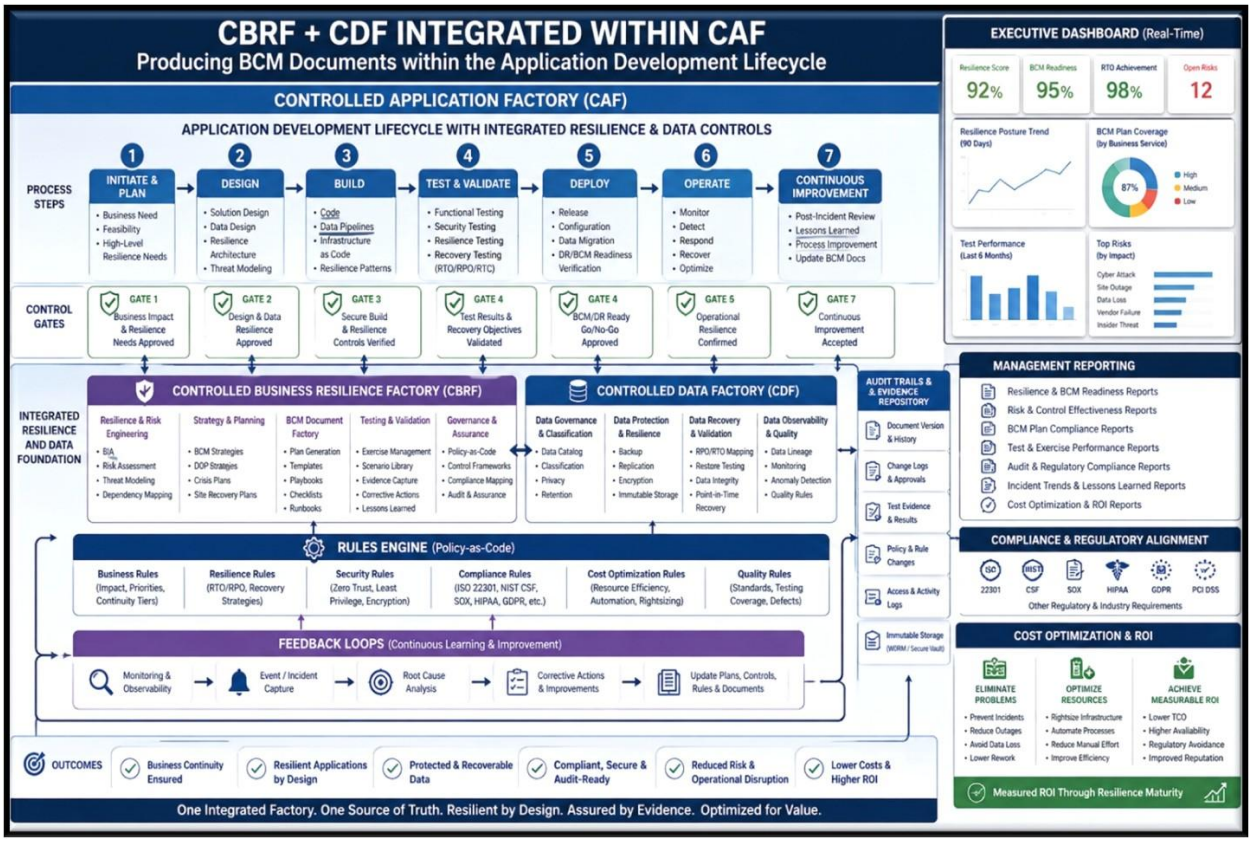
Thomas Bronack, President

Data Center Assistance Group, LLC

bronackt@dcag.com | bronackt@gmail.com | https://www.dcag.com | (917) 673-6992

# White Paper: Enterprise Secure Resilience and Continuity Operating Model

Integrating Business Continuity Management (BCM), Continuity of Operations (COOP), Disaster Recovery (DR), Crisis Management, Site Recovery, and Vendor Continuity Management




Aligned with Controlled Application Factory (CAF), Controlled Data Factory (CDF), and Controlled Business Resilience Factory (CBRF)

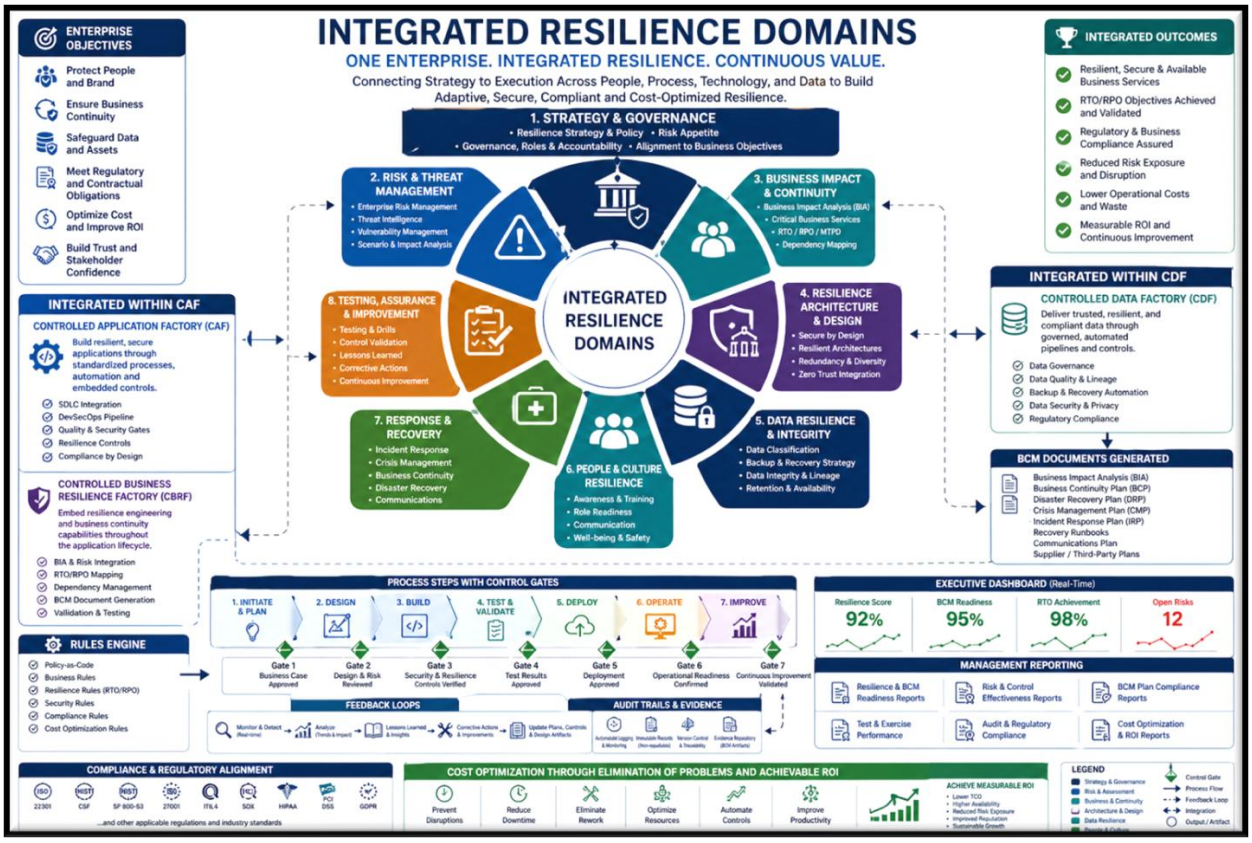
## Executive Summary

Organizations face increasingly complex disruptions that affect technology, facilities, personnel, suppliers, customers, and regulators simultaneously. Traditional resilience programs often address only isolated dimensions such as IT disaster recovery while overlooking business continuity, continuity of operations, crisis leadership, site relocation, vendor continuity, and operational recovery.

This white paper defines an integrated Enterprise Secure Resilience and Continuity Operating Model combining BCM, COOP, DR, Crisis Management, Site Recovery, Vendor Continuity Management, Cyber Resilience, and Operational Resilience aligned with the Controlled Application Factory (CAF), Controlled Data Factory (CDF), and Controlled Business Resilience Factory (CBRF).

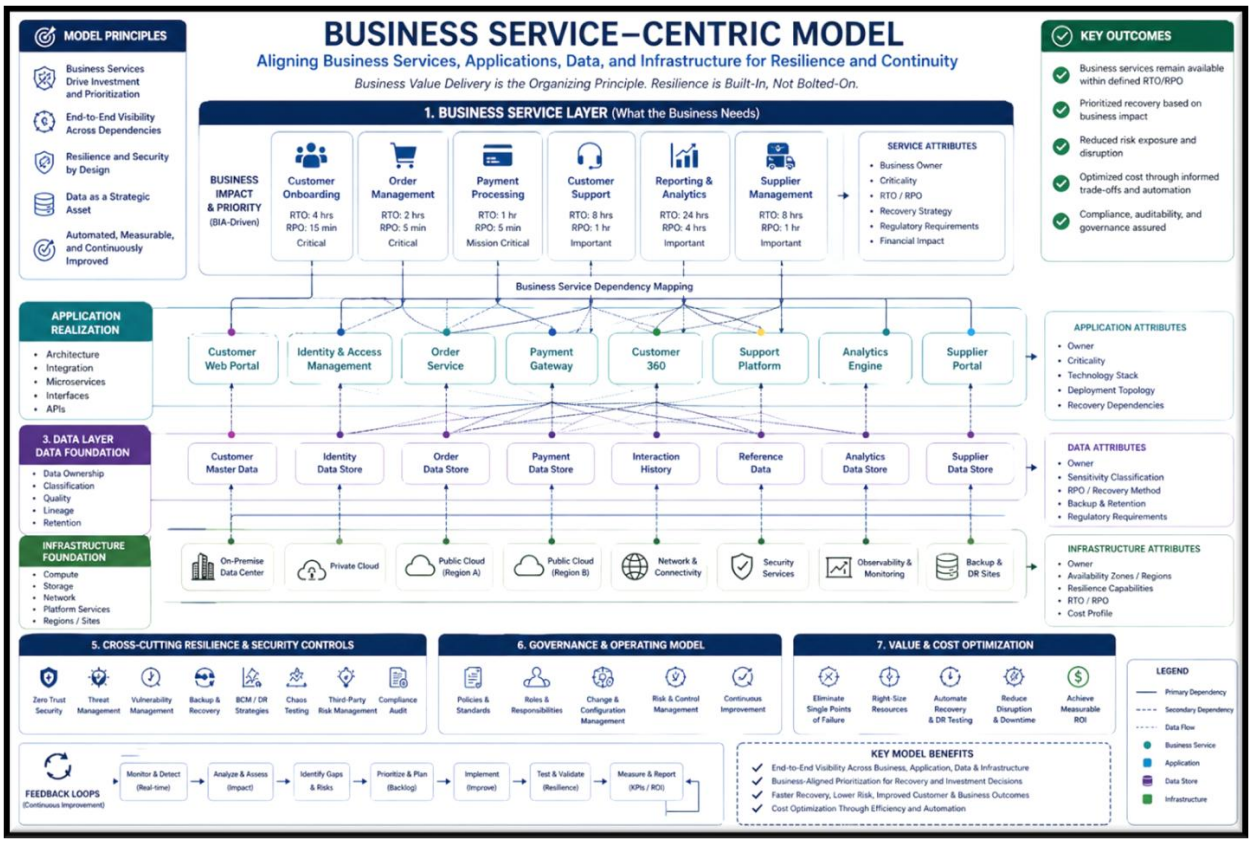
### 1. Integrated Resilience Domains

- Business Continuity Management (BCM)
- Continuity of Operations (COOP)
- Disaster Recovery (DR)
- Crisis Management (CM)
- Site Recovery (SR)
- Vendor Continuity Management (VCM)
- Cyber Resilience
- Operational Resilience



**2. Business Service-Centric Model**

All resilience planning should align to critical business services and their dependencies across people, process, technology, facilities, and vendors.




**3. Business Continuity Management (BCM)**

BCM ensures critical business processes continue through alternate procedures, remote work, alternate staffing, and alternate suppliers.

**4. Continuity of Operations (COOP)**

COOP ensures mission-essential functions continue through succession planning, delegation of authority, alternate operating locations, and vital records management.

**5. Disaster Recovery (DR)**

DR restores applications, infrastructure, networks, and data. Recovery Time Capability (RTC) must be measured against RTO and RPO.

**6. Crisis Management**

Crisis Management provides executive command, communications, escalation, and stakeholder coordination.

**7. Site Recovery**

Site Recovery ensures facilities can be restored or relocated through hot, warm, cold, reciprocal, or remote-work models.

**8. Vendor Continuity Management**

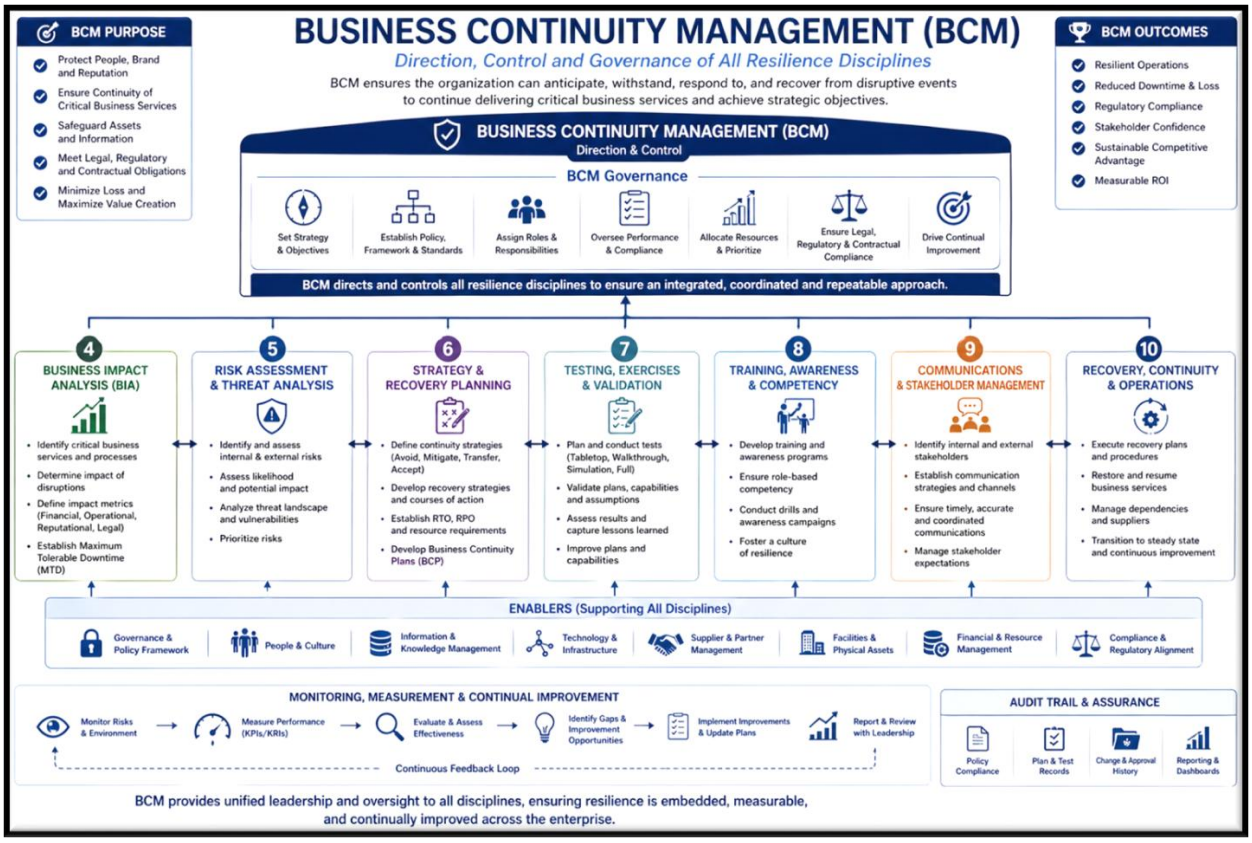
Vendors must redirect deliveries to alternate sites and maintain supply continuity during disruptions.

**9. Site Security and Restoration**

Post-incident site protection must be maintained after first responders leave. Contracts should exist for security, salvage, and restoration providers such as BELFOR, SERVPRO, and ServiceMaster Restore.

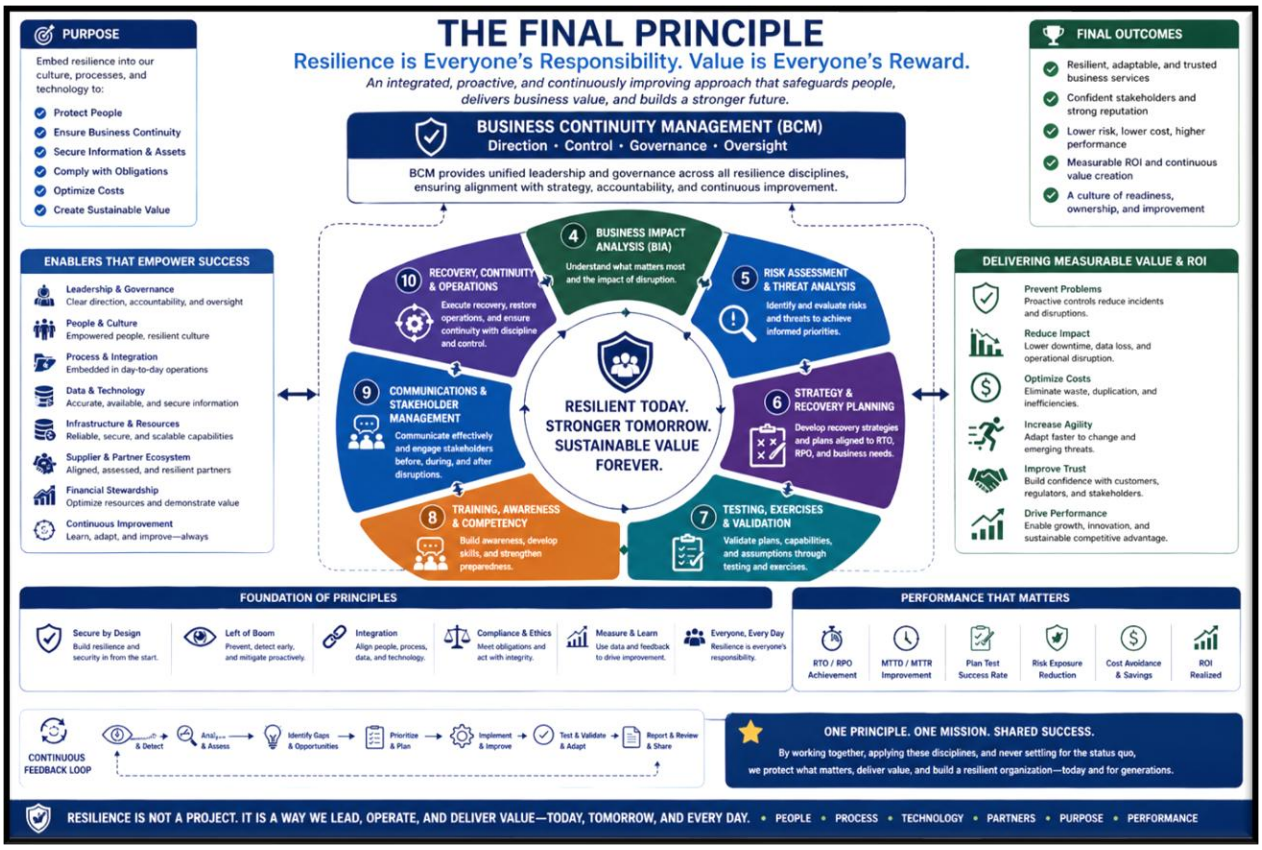
**10. Governance and Testing**

Resilience controls should be embedded into CAF, CDF, and CBRF pipelines and validated through exercises and evidence collection.



**11. Final Principle**

No critical business service should enter or remain in production unless continuity, recovery, crisis, vendor, and site recovery plans are approved and tested.




**12. Call to Action**

Should you find the information contained within this White Paper of interest to you and you believe DCAG can assist your company achieve the goals outlined in this paper, please contact us to schedule a discussion and potential contract for our services. Please contact:

Thomas Bronack, President

Data Center Assistance Group, LLC

bronackt@dcag.com | bronackt@gmail.com | https://www.dcag.com | (9170 673-6992