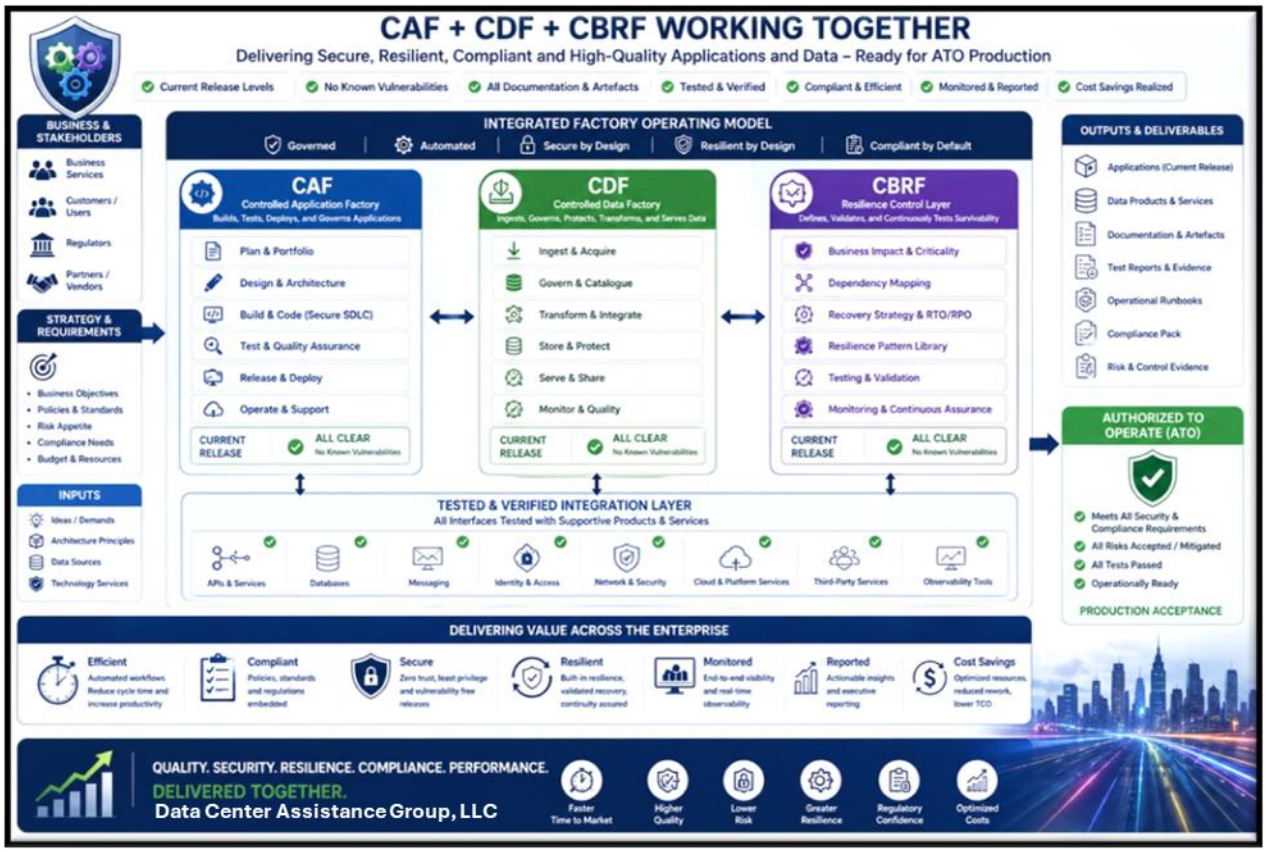
The Controlled Enterprise Factory™

Integrating Application, Data, and Resilience for Secure, Compliant, and Automated Delivery



Created by

Thomas Bronack, President

Data Center Assistance Group, LLC

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

Table of Contents

Contents

A. Secure Resilience Model Aligned with CAF and CDF

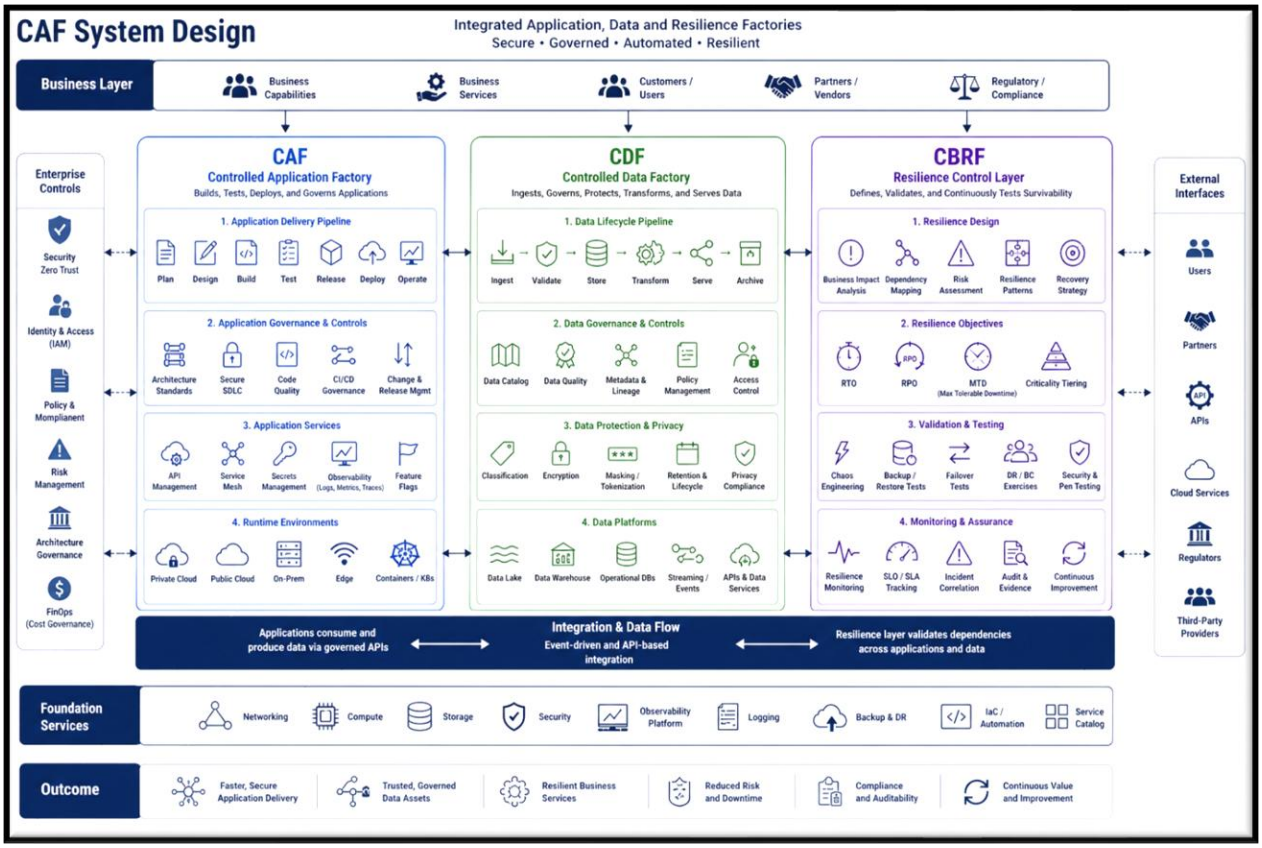
1. Core Operating Model

CBRF: Controlled Business Resilience Factory sits alongside:

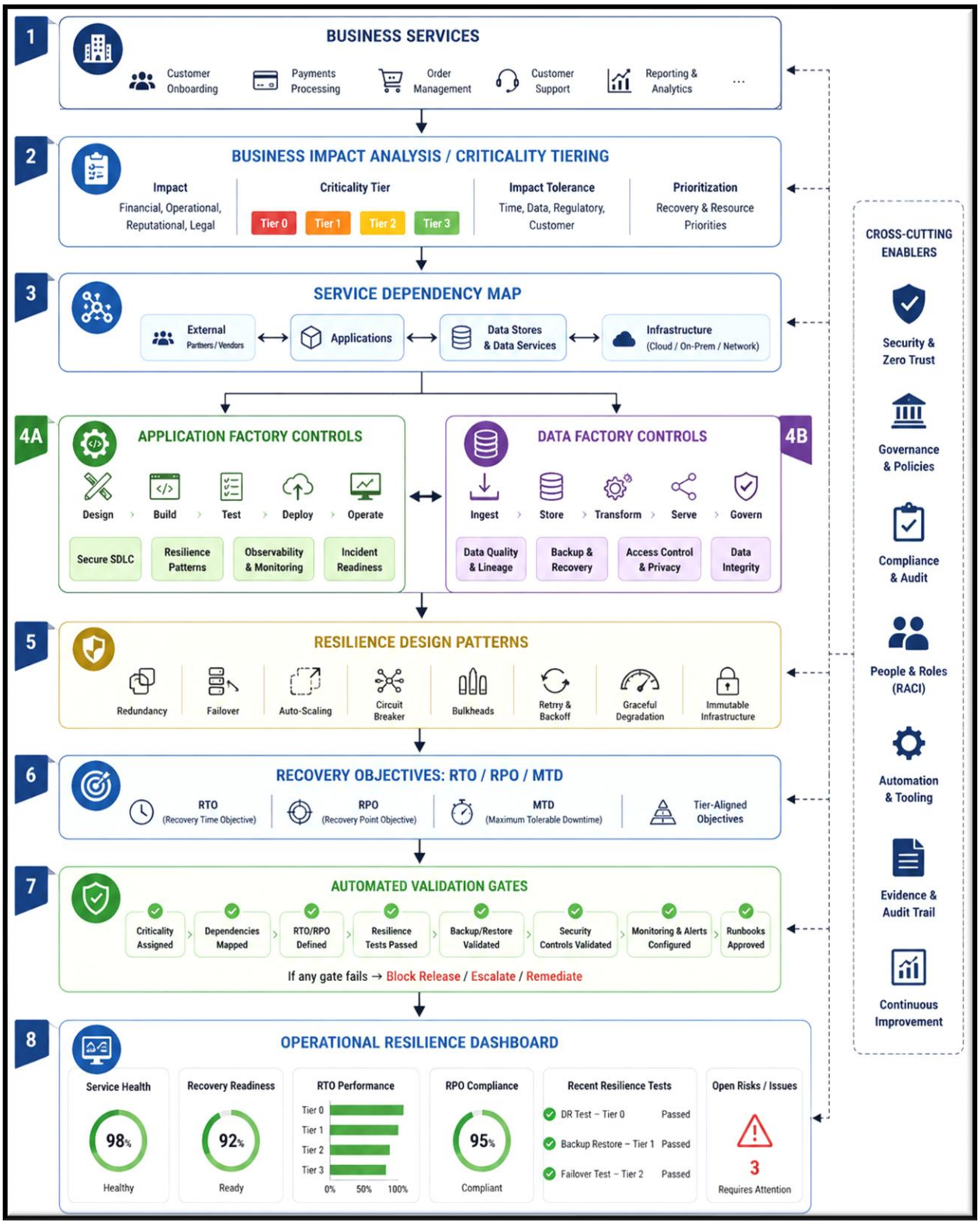
- **CAF:** Controlled Application Factory
  Builds, tests, deploys, and governs applications.
- **CDF:** Controlled Data Factory
  Ingests, governs, protects, transforms, and serves data.
- **CBRF:** Resilience control layer
  Defines, validates, and continuously tests survivability of business services, applications, data flows, and operational dependencies.

The model should treat resilience as a **factory control plane**, not a post-deployment continuity exercise.

Controlled Application Factory (CAF) System Design overview



2. Target Architecture – CAF with CBRF and CDF



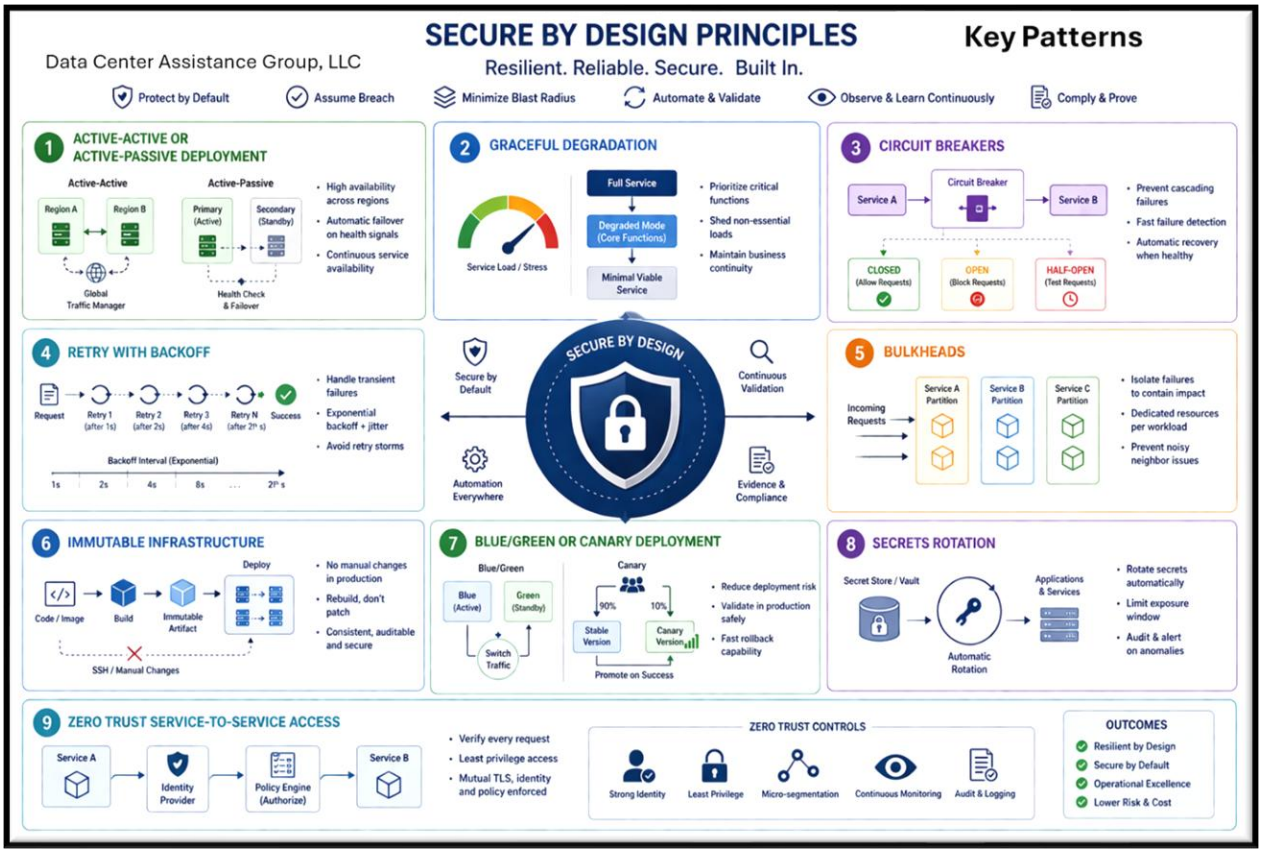
3. Resilience Control Domains

a. Business Service Resilience

Each business service should have:

Control	Purpose
Business Impact Analysis	Defines criticality and impact tolerance
RTO / RPO / MTD	Sets recovery expectations
Dependency Map	Links apps, data, APIs, vendors, infrastructure
Minimum Viable Service	Defines degraded-mode operation
Recovery Strategy	Documents failover, restore, workaround, manual procedures

b. CAF Integration Controls



Embed resilience directly into the application delivery pipeline.

CAF Stage	Required Resilience Control
Architecture	Resilience pattern selection
Design	Threat-informed failure-mode analysis
Build	Secure coding, retry logic, circuit breakers
Test	Chaos testing, backup restore testing
Release	RTO/RPO validation gate
Operate	Observability, incident playbooks, SLO monitoring

Key patterns:

- Active-active or active-passive deployment
- Graceful degradation
- Circuit breakers
- Retry with backoff
- Bulkheads
- Immutable infrastructure
- Blue/green or canary deployment
- Secrets rotation
- Zero Trust service-to-service access

c. CDF Integration Controls

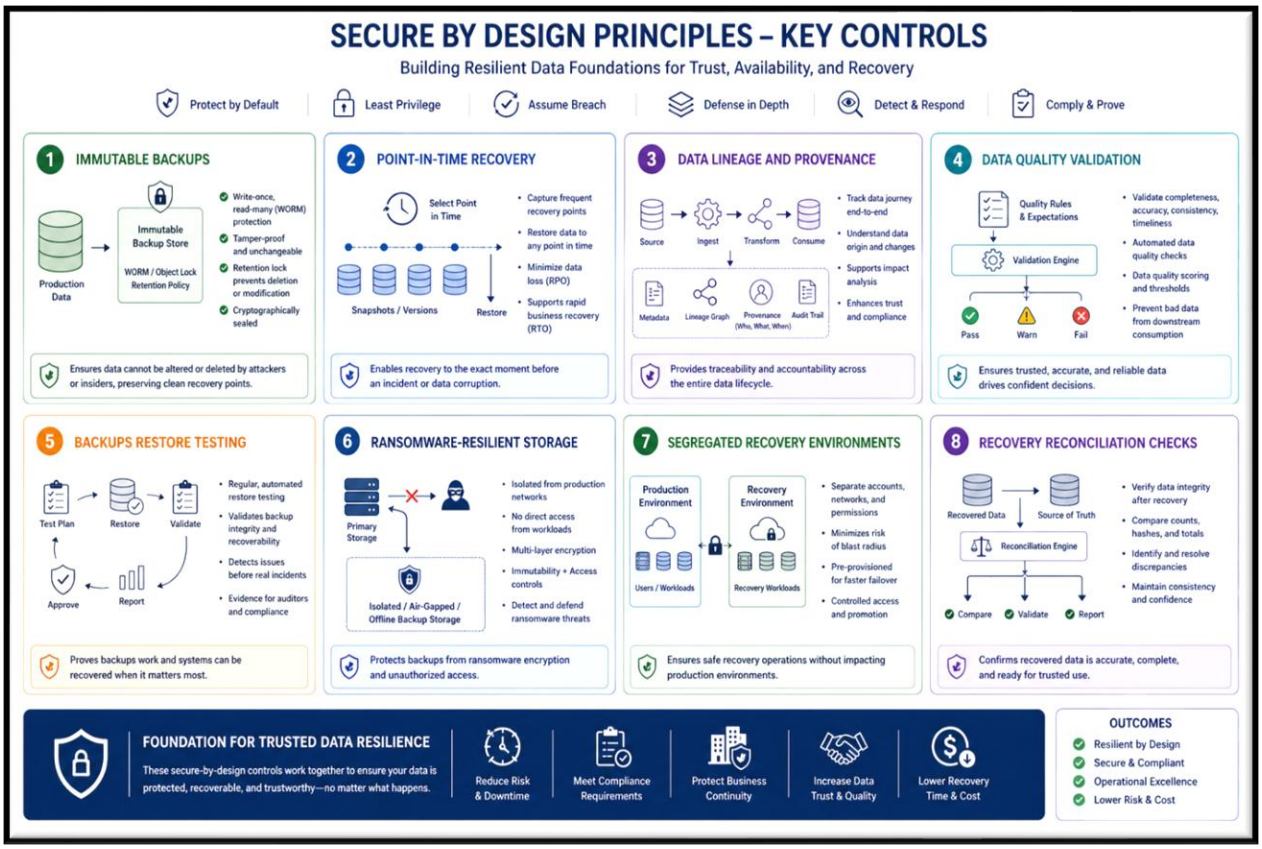
Data resilience must be treated separately from application availability.

CDF Stage	Required Resilience Control
Ingest	Source validation and replay capability
Store	Encryption, immutability, retention policy
Transform	Lineage, validation, rollback checkpoints
Serve	Access control, data quality SLOs
Recover	Backup, restore, reconciliation, integrity checks

Key controls:

- Immutable backups
- Point-in-time recovery
- Data lineage and provenance
- Data quality validation
- Backups restore testing
- Ransomware-resilient storage
- Segregated recovery environments
- Recovery reconciliation checks

d. Secure by design key controls



4. Criticality Tiering Model

Tier	Example	RTO	RPO	Pattern
Tier 0	Life/safety, payment clearing, identity	Minutes	Near-zero	Active-active
Tier 1	Revenue-critical platforms	< 4 hrs	< 1 hr	Warm standby
Tier 2	Important business operations	< 24 hrs	< 8 hrs	Backup/restore
Tier 3	Administrative services	2–5 days	24 hrs+	Manual recovery

5. Secure-by-Design Resilience Gates

Every CAF/CDF release should pass these gates:

1. **Business criticality assigned**
2. **RTO/RPO defined and approved**
3. **Application and data dependencies mapped**
4. **Failure modes documented**
5. **Security controls validated**
6. **Backup and restore tested**
7. **Monitoring and alerting configured**

8. **Incident and recovery playbooks created**
9. **Access controls reviewed**
10. **Resilience evidence stored for audit**

No production release should proceed without minimum resilience evidence.

6. Governance Model

a. Required Roles

Role	Responsibility
Business Service Owner	Owns impact tolerance and recovery priority
Application Owner	Owns CAF resilience controls
Data Owner	Owns CDF recovery and integrity
Security Architect	Validates secure-by-design controls
Resilience Architect	Owns CBRF patterns and testing
SRE / Operations	Owns observability and recovery execution
Risk / Compliance	Validates evidence and policy alignment

7. Resilience Evidence Repository

CBRF should produce reusable, auditable artifacts:

- Business Impact Analysis
- Service dependency map
- Application recovery design
- Data recovery design
- RTO/RPO matrix
- Backup validation report
- Disaster recovery test evidence
- Security control mapping
- Incident response playbook
- Recovery runbook
- Exception register
- Residual risk statement

8. Control Framework Mapping

Principle	CBRF Implementation
ISO 22301	Business continuity lifecycle
NIST CSF	Identify, Protect, Detect, Respond, Recover
NIST SSDF	Secure resilience embedded in SDLC
Zero Trust	Least privilege recovery paths
ITIL	Incident, problem, change, continuity processes
Cloud Well-Architected	Reliability and security validation
Left of Boom	Preventive controls before disruption

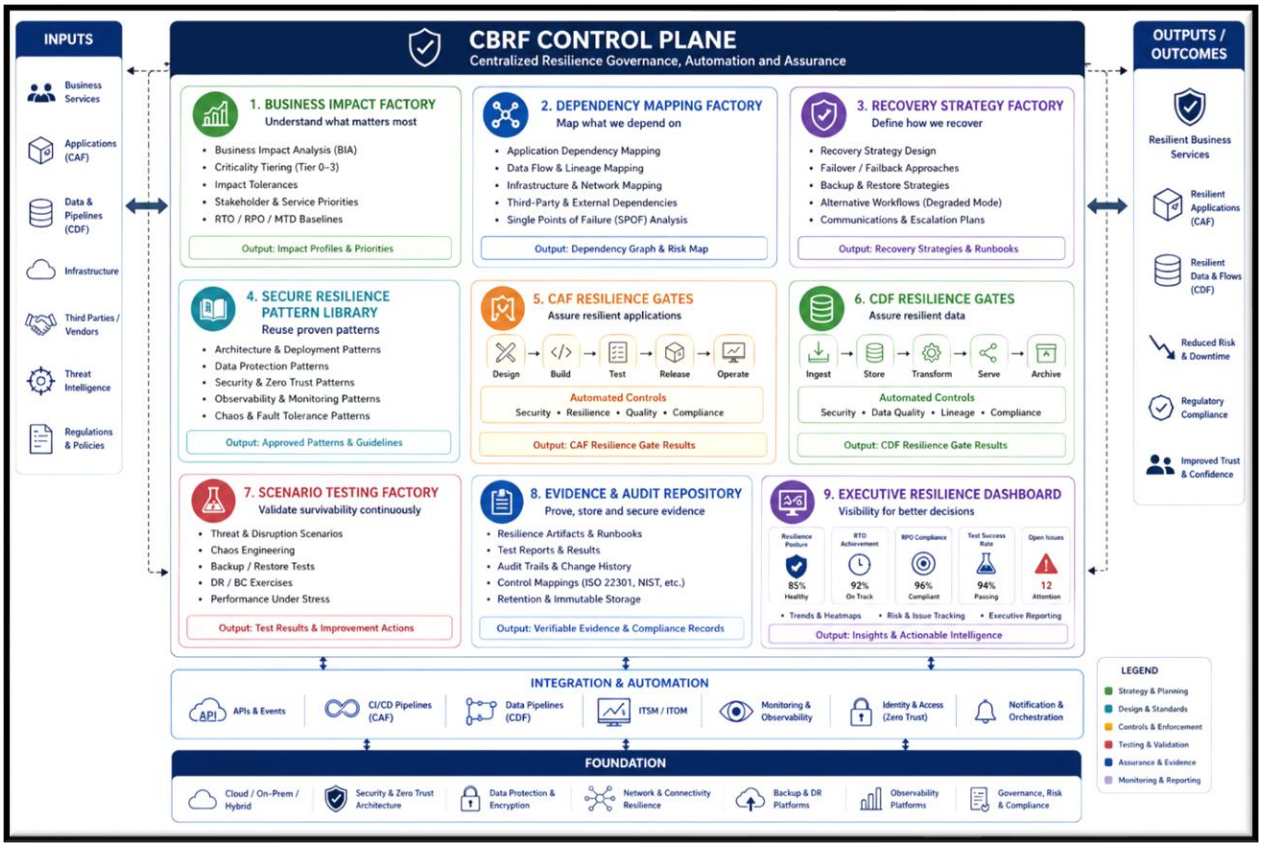
9. Devil's Advocate Risks

Watch for these failure points:

- Applications marked "resilient" while their data stores are not
- RTOs defined by IT without business approval
- Backups created but never restored
- Failover procedures requiring privileged access that is unavailable during crisis
- Data pipelines with no replay capability
- Vendor dependencies excluded from recovery planning
- Shared services becoming hidden single points of failure
- Resilience controls bypassed for "urgent" releases

10. Recommended Reference Model

a. CBRF Control Plane



The target outcome is a **repeatable, governed, secure resilience factory** where business continuity, application resilience, data recoverability, and cybersecurity controls are engineered into delivery pipelines rather than tested after deployment.