RESILIENCE IS THE NEW COMPLIANCE

A Leadership Overview of the Resilience Operating Model (ROM)

Executive Brief — Advance Release of the Resilience Operating Model

Oritse J. Uku
Cybersecurity & Resilience Executive
Executive Brief • December 2025

The views expressed are solely the author’s and do not represent any affiliated organization.

Why Resilience Is the New Compliance

Enterprises now operate in an era defined by volatility. Technology ecosystems have become vast, deeply interdependent, and often opaque. Critical services rely on global supply chains, cloud concentration points, and identity-driven architectures that evolve faster than traditional assurance models can track. Disruptions that were once exceptional now cascade across third-parties and critical infrastructure with speed and scale.

Identity-driven architectures, the layer governing authentication, authorization, and service-to-service trust across cloud and on-prem systems, have become foundational. Yet most organizations still assess them through periodic control reviews, rather than continuous performance evidence.

For two decades, compliance served as the dominant line of defense. Organizations proved that controls were designed, documented, and periodically tested. However, recent systemic outages reveal a structural gap: even fully compliant institutions experience failures in their most important services. Controls are designed to demonstrate intent, not to guarantee continuity.

Regulators around the world have taken notice.

Supervisors across the United Kingdom, European Union, Australia, Singapore, Canada, and the United States now expect firms to demonstrate that critical services can remain within tolerance during severe, but plausible, disruption. This shift represents a profound reorientation of oversight philosophy. Compliance is no longer enough to establish trust. **Evidence of performance under stress is becoming the new standard.**

Resilience is emerging not as a control domain, but as a strategic capability — a measure of whether an organization can continue delivering the outcomes that matter most to customers, markets, and society, even as critical dependencies fail. This is why resilience is becoming the new compliance: it reflects **not what an organization has documented, but what it can demonstrably sustain under real-world conditions.**

> *“Resilience is emerging not as a control domain, but as a strategic capability.”*

The views expressed are solely the author’s and do not represent any affiliated organization.

Where Traditional Operating Models Fail

Modern enterprises are structurally complex. Cybersecurity, technology operations, enterprise risk management, business continuity, disaster recovery, and third-party oversight all operate through their own taxonomies and execution rhythms. These functional silos create blind spots in how the enterprise understands and manages continuity risk.

Disruptions do not respect organizational boundaries. Yet most resilience disciplines were built inside them.

This fragmentation has real consequences. Technology teams measure reliability in terms of infrastructure uptime; business leaders evaluate performance through customer experience and financial continuity. Cybersecurity seeks to minimize exposure through controls; operational teams optimize for speed and delivery. Third-party functions focus on contractual assurance, not operational viability. Risk management concentrates on policy alignment and governance.

Each discipline has its own definition of “criticality,” often derived from unrelated criteria.

These divergences become undeniable during real-world incidents. Architectural dependencies surface only when they break. Recovery plans that exist on paper fail in practice. Critical processes lack clear ownership. Shared platforms and cloud concentration risks become visible only under stress. Despite substantial investment, most institutions still struggle to produce evidence that their essential services can remain within acceptable limits.

The challenge is not the absence of frameworks. It’s the absence of cohesion. Enterprises require a unifying operating system that integrates the disciplines supporting outcome-based resilience and aligns them toward a single objective: **continuity of critical services.** Without this, compliance remains disconnected from performance.

The Global Oversight Convergence

Regulatory language differs across jurisdictions, but supervisory expectations are converging in substance.

- The **United Kingdom's PRA SS1/21** centers on identifying important business services, setting impact tolerances, mapping dependencies, and testing against severe, but plausible, disruptions.
- **Europe's Digital Operational Resilience Act (DORA)** codifies similar expectations for financial institutions and their critical third-parties.
- **Australia's CPS 230** elevates operational risk and resilience with equal weight.
- **Singapore, Canada,** and the **United States** have aligned their supervisory frameworks around comparable principles.

The supervisory message is unified: **regulators are moving from documentation-centric assurance to performance-based evidence.**

Firms must demonstrate that critical services can remain within tolerance even when key components fail. Boards are being held directly accountable for resilience oversight. Institutions unable to produce reliable, machine-verifiable performance evidence face heightened scrutiny, expanded testing expectations, and reputational pressure.

This convergence is reshaping how directors and executives think about resilience. Continuity is no longer a back-office function. It is a strategic capability that influences competitiveness, investor confidence, transformation outcomes, and regulatory trust.

The views expressed are solely the author's and do not represent any affiliated organization.

Why Enterprises Need an Operating System, Not Another Framework

Enterprises do not lack frameworks. They have dozens — cybersecurity standards, IT service management, business continuity, risk governance, audit requirements, cloud control baselines, third-party assurance, crisis management, and data governance.

Yet operational fragility persists.

Frameworks function as policy systems, not execution systems. They define what “good” looks like, but rarely connect governance to real-time performance. They produce pockets of maturity that do not translate into enterprise-wide resilience. They incentivize local optimization, not systemic reliability.

> *“Frameworks are policy systems. Resilience requires an operating system.”*

What organizations require is something different: **an operating system** — one that unifies the disciplines needed to achieve and demonstrate resilience. An operating system coordinates accountability, standardizes definitions, aligns incentives, enables shared situational awareness, and generates evidence-based insights. It ensures the enterprise understands what is critical, how it functions, what it depends on, and how it behaves under stress.

Without such a system, resilience becomes episodic — governed by annual tests, policy cycles, or audit reviews. But resilience is inherently continuous. It must adapt to architectural drift, vendor ecosystem changes, geopolitical shifts, and evolving business models.

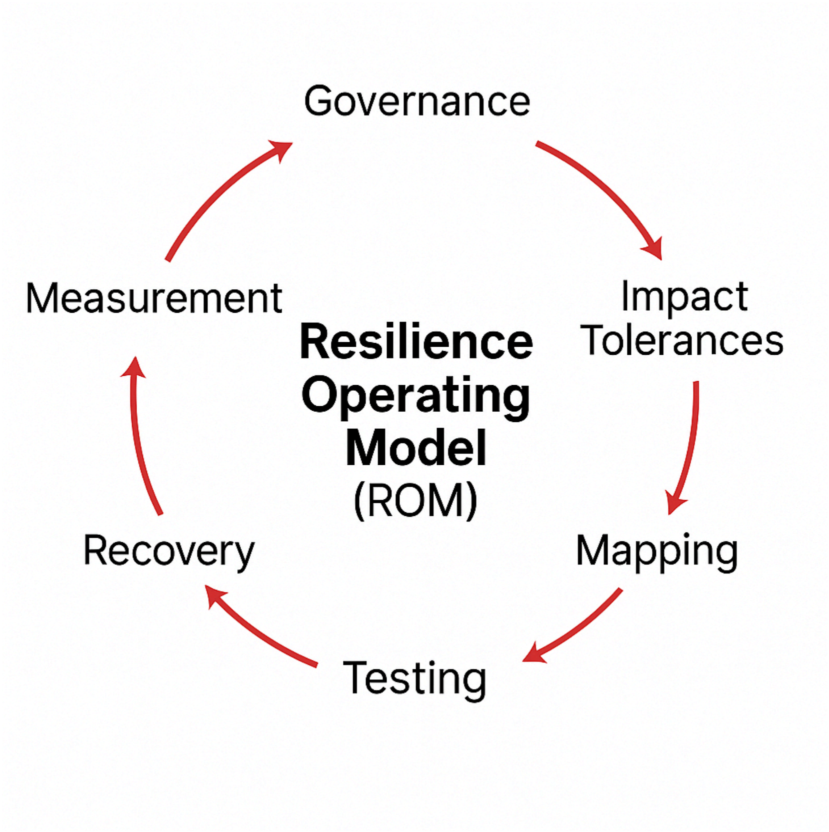
The **Resilience Operating Model (ROM)** is designed to meet that need.

The views expressed are solely the author’s and do not represent any affiliated organization.

The Resilience Operating Model (ROM)

The ROM is a unified management system for operational resilience. It integrates governance, risk, technology, cybersecurity, continuity, and assurance into a single operating rhythm. **It does not replace existing frameworks; it organizes them into a coherent, measurable performance discipline.**

The ROM consists of six interconnected pillars that form a closed-loop system:



Governance

Establishes clear executive ownership, decision rights, and board oversight. Resilience becomes a shared fiduciary responsibility across the CRO, CIO, and CISO — creating leadership alignment capable of managing complexity.

The views expressed are solely the author’s and do not represent any affiliated organization.

Impact Tolerances

Define the thresholds beyond which harm becomes unacceptable, measured through duration, volume, degradation, or other quantifiable parameters. These tolerances anchor the ROM and shape prioritization and testing.

Mapping

Provides structural transparency into how each important business service functions. It traces the full chain of dependencies — technology components, cloud services, identity systems, data paths, facilities, and third-parties. In modern architectures, mapping incorporates telemetry from cloud and observability tooling, ensuring the model reflects reality, rather than static documentation. Mapping is not inventory; it is a living operational model.

Testing

Validates whether a service behaves as expected under stress. This includes technical failover, dependency stress scenarios, cyberattack simulations, and business-service continuity exercises. In cloud-native environments, it requires validating service-level objectives across accounts, regions, and identity layers. Leading institutions incorporate automated chaos testing and AI-driven scenario selection to surface failure modes traditional exercises miss.

Recovery

Ensures the organization can restore continuity within tolerance. Recovery is measured by the reestablishment of service outcomes, not by the restoration of individual components.

Measurement

Converts resilience from narrative to quantifiable discipline. Metrics track how critical services perform under stress and whether they are becoming more stable or more fragile. Increasingly, these insights derive from automated evidence — cloud telemetry, observability pipelines, recovery-path validation, and real-time dependency analytics. This enables **continuous validation** as part of normal operations, not periodic assessments.

Together, these capabilities make resilience observable, testable, governable, and improvable.

The views expressed are solely the author's and do not represent any affiliated organization.

The Leadership Shift

Implementing the ROM is not a technical exercise. It’s a leadership shift.

- **For CEOs**, resilience becomes a strategic asset that safeguards transformation, customer trust, and enterprise value.
- **For CROs**, it integrates risk appetite with real-time operational limits.
- **For CIOs**, resilience reframes technology design through architecture determinism — ensuring systems behave predictably under stress, with controlled failover, validated recovery paths, and reliable dependency performance.
- **For CISOs**, it elevates the role from assurance to enterprise resilience leadership, unifying cyber and operational performance.
- **For boards**, it provides clear evidence of continuity risk, transforming oversight from compliance review to performance dialogue.

This shift requires aligned incentives, transparent limitations, and a willingness to validate assumptions through testing. When leadership embraces this model, resilience becomes a performance differentiator — reducing volatility, strengthening transformation, and enhancing trust across regulators, customers, and markets.

What Comes Next

Supervisory expectations will intensify. Digital ecosystems will grow more interdependent, dependencies more opaque, and disruptions more consequential.

Regulators are already signaling future direction:

- Assurance for AI systems
- Real-time resilience telemetry
- Expanded oversight for critical third-parties
- Cross-domain scenario testing

Institutions unable to demonstrate real resilience — not program maturity — will face increasing scrutiny and strategic constraints.

Those that adopt a unified operating model will position themselves differently. They will reduce operational volatility, improve recovery predictability, strengthen regulatory relationships, and protect customer trust. They will execute transformation with greater confidence.

Resilience is becoming the new compliance because **reliability is the ultimate measure of trust**. The ROM provides the system through which that reliability can be governed, demonstrated, and continually improved.

The views expressed are solely the author's and do not represent any affiliated organization.

Call to Action: What Leaders Should Do Now

The shift from compliance to resilience is real and accelerating. Institutions cannot wait for the next supervisory paper — or the next disruption — to begin this work.

Begin with clarity.

Identify the small set of services whose failure would create material harm. Treat these as the enterprise’s continuity benchmark. This realignment alone often reveals the gap between perceived and actual resilience.

Interrogate your evidence.

For each critical service, determine what proof exists that it can remain within tolerance during a severe, but plausible, disruption. Not documentation. Not maturity scores. **Evidence** — testing logs, dependency performance data, validated recovery paths, scenario results. Absence of evidence is your signal to act.

Align your leadership.

Resilience is not owned by a single function. The CRO, CIO, and CISO must operate as a unified triad, supported by operations, business leadership, and the board. Establish a shared view of what “within tolerance” means, where the organization is exposed, and what is required to demonstrate continuity with confidence.

These steps form the foundation of the Resilience Operating Model. They do not require full implementation to create immediate value. They require only intention, alignment, and the willingness to replace assumptions with evidence.

Organizations that take these steps now will shape the next era of operational excellence, where resilience is demonstrated, measurable, and trusted.

The full white paper, forthcoming, will provide the detailed architecture for building and sustaining the ROM. However, the work can begin today.

> *“Evidence, not documentation, is the new foundation of resilience.”*

The views expressed are solely the author’s and do not represent any affiliated organization.