From Minimum Viability to Operational Resilience

A Framework for Continuous Business

By **David Nowak**, Principal, Deloitte Cyber Defense & Resilience and **Bill O'Connell**, Chief Security Officer, Commvault

READIVERSE

Commvault®

Executive Summary

Commvault + Deloitte.

Ask a CISO whether their organization can recover from a serious cyberattack. Most will say “yes.” Ask them to prove it – right now, for each of their most critical business services, within the timeframes their board believes are achievable, and the answer changes.

That gap between confidence and evidence is the central challenge of cyber resilience today. And it is the problem that resilience operations (ResOps) is designed to solve.

Our earlier joint work established minimum viability as the foundation: the discipline of identifying and protecting the essential operational state a business must restore to function during and after a cyberattack. Minimum viability answers the question of what must come back first. ResOps answers the harder question: How do you restore to normal business operations, reliably, under pressure, every time? And how do you prove it?

This paper sets out why resilience programs fail when treated as compliance exercises rather than operating models, how the ResOps discipline addresses that failure, and how Commvault and Deloitte together help organizations make the shift from assurance to evidence.

Why Resilience Programs Fail

Commvault + Deloitte.

$400 billion

lost annually by Global 2000 companies to unplanned downtime: 9% of profits[1]

1. The Hidden Costs of Downtime, Splunk

Most organizations have disaster recovery plans, backup policies, and incident response runbooks. The documentation exists. The assurances are on file. But documentation does not execute itself.

When a ransomware attack encrypts production systems at 2 a.m., the plan last exercised by a different team against a different architecture meets reality. Dependencies that were never mapped, surface as blockers. Backup copies never verified contain the malware that started the incident.

The structural problem is organizational. Resilience treated as a program, reviewed periodically, and reported on by exception becomes disconnected from how systems, people, and threats actually evolve. The plan stays static while everything around it changes.

Disruption-ready organizations have learned that resilience is not a project to complete or a document. It is an operating condition that must be actively maintained, continuously tested, and governed with the same discipline as any other business-critical capability.

Cyberattacks compound this challenge in a specific way. For decades, disaster recovery assumed backups were trustworthy. Ransomware invalidates that assumption – adversaries now specifically target backup infrastructure. This is why the three disciplines of cyber resilience address fundamentally different questions:

- Cybersecurity asks: Are we under attack?
- Backup and disaster recovery ask: Do we have copies?
- ResOps asks: Can we actually return to normal business operations, for each critical service, right now?

Organizations that conflate these, assuming that an adequate disaster recovery program provides cyber recovery capability, are exposed in ways they may not discover until they are inside an active incident.

The regulatory stakes make this urgent. Frameworks like the EU's Digital Operational Resilience Act (DORA) require organizations to define impact tolerances for critical services and demonstrate through testing that those tolerances can be met. SEC rules require material incident disclosure within four business days. Boards are asking the same question in plain language: If we were breached tonight, could we keep our promises to customers? Not in theory – in practice.

From Minimum Viability to ResOps

Commvault + Deloitte.

Minimum viability defines the essential operational state a business must restore to function during and after a cyberattack. It is the business-defined answer to: What must come back first? A manufacturer prioritizes production line controls. A healthcare system prioritizes patient care and electronic health records. A financial institution prioritizes transaction processing and fraud detection.

Minimum viability defines the destination. ResOps is the discipline that enables the organization to reach it, reliably and provably, every time it matters.

ResOps unites security, infrastructure, and operations teams around critical services, resilient system design, and continuous validation, so organizations can withstand disruption and recover within defined impact tolerances, and prove it with evidence. It is important to be precise: ResOps is not a product or a SKU. It is an operational discipline that must be adopted across engineering, security, operations, and service delivery.

The Six Domains of ResOps:

01 Resilience governance

Define what must be protected, executive buy-in, how much disruption is tolerable, and who owns accountability. Align funding to tested impact tolerances, track resilience gaps in the risk register, and report recovery posture to the board every quarter.

02 Recovery planning

Know exactly what must survive and what it depends on. Map critical services and business processes to their underlying core IT infrastructure and services, applications, data, identities, and third parties. Establish the impact tolerances that drive every subsequent architecture and investment decision.

03 Recovery architecture

Limit blast radius and protect recovery paths through defense-in-depth and hardened, isolated protection domains for backups and recovery assets. Design for controlled degradation, not catastrophic failure – and for rebuild from scratch, when it comes to that.

04 Recovery assurance

Turn assumptions into evidence through a continuous exercise portfolio for example: executive and technical tabletops, monthly game days, bi-annual live recovery drills, and third-party failover tests. Validate that critical services can be restored within defined impact tolerances.

05 Continuous improvement

Close the loop between validation and action. Feed findings from exercises, Service Resilience Indicator (SRI) trends, and incident reviews into a governed resilience backlog – prioritized improvements owned by specific service teams and tracked through normal governance processes until resolved.

Impact Tolerances, SRIS, And Mean Time To Clean Recovery

Three metrics bridge technical recovery capability and board-level accountability.
Together, these three metrics transform resilience governance from periodic assurance into continuous accountability.

Impact tolerances

Define the maximum duration and data loss a critical service can sustain before consequences become unacceptable. Unlike recovery time objectives (RTO) and recovery point objectives (RPO), which are set by IT, impact tolerances are set by business leaders and used to drive recovery architecture and investment.

Service Resilience Indicators (SRIs)

Extend this into ongoing measurement – quantifiable signals drawn from testing results, dependency analysis, and operational telemetry that show whether a service's recoverability is within, approaching, or outside its defined tolerance.

Mean Time to Clean Recovery (MTCR)

Addresses the question RTO and RPO leave unanswered: Can you trust the data you are restoring? Where RTO measures speed and RPO measures data loss, MTCR measures how long it takes to restore data that is verifiably clean – making integrity a measurable recovery objective, not an assumption.

The Resops Maturity Model

Maturity is measured not by tools deployed or documents produced, but by the ability to demonstrate recoverability with evidence and use that evidence to drive decisions.

Level	Characteristics	Outcome
Level 0 **Fragmented Recovery**	Capabilities exist in isolation. Critical services are undefined, dependencies incomplete, and recovery relies on manual effort. Impact tolerances are undefined.	Recovery may succeed, but only through improvisation and luck.
Level 1 **Basic Discipline**	Critical services identified, basic objectives exist, but end-to-end evidence is incomplete. Confidence is based more on plans than proof.	The organization believes it can recover but cannot demonstrate it.
Level 2 **Integrated ResOps**	Cross-functional discipline established. Impact tolerances and SRIs defined. Scenario-based validation performed regularly. Gaps flow into a managed backlog.	Can demonstrate recoverability for critical services in known scenarios.
Level 3 **Evidence-Driven**	Resilience continuously validated as a business capability. Evidence guides investment, change approval, and board decisions. Rebuild from scratch is feasible.	Resilience is measured, governed, and improved continuously – not assumed.

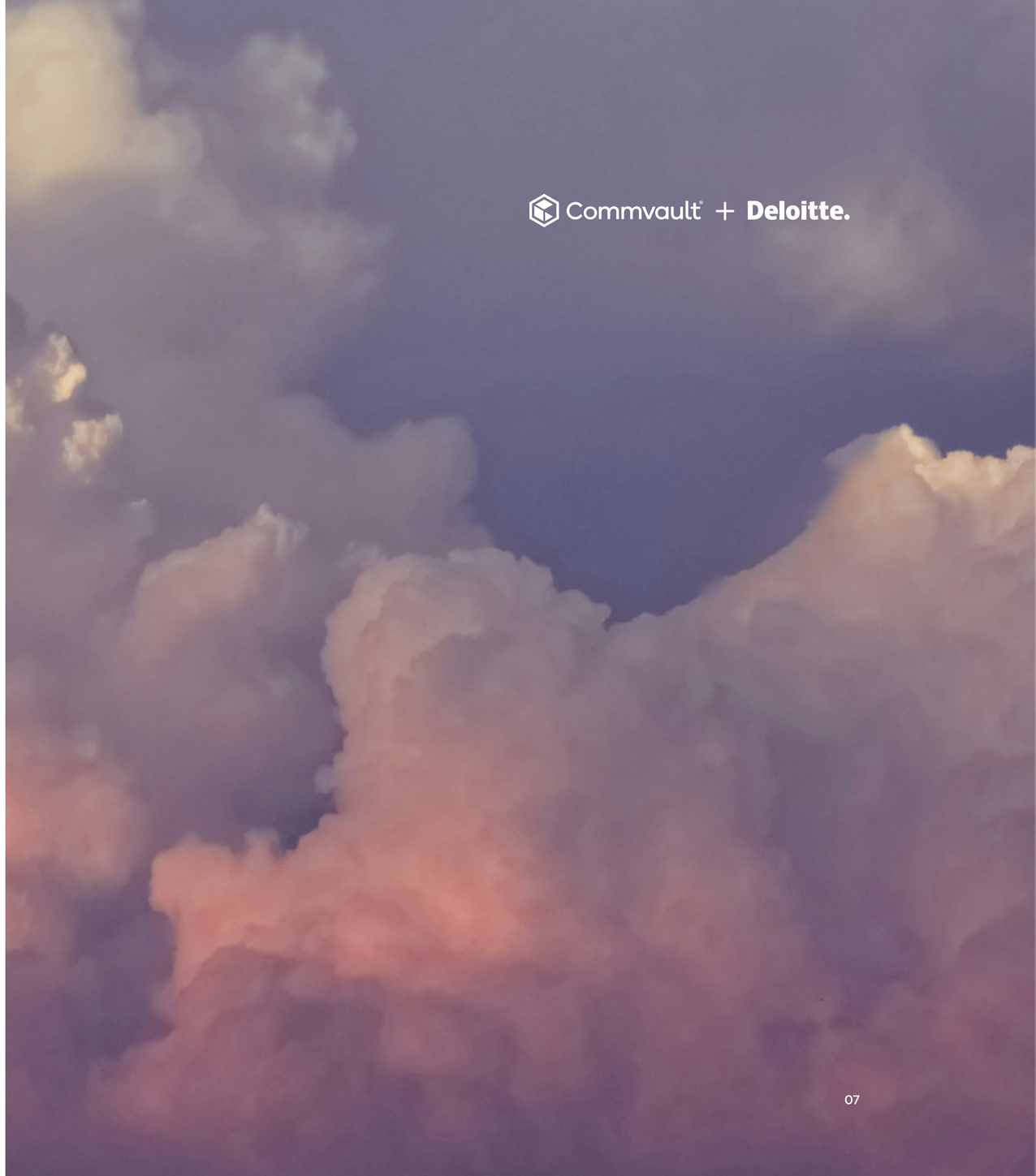
How Deloitte Helps

Making the shift from resilience-as-program to ResOps-as-operating-model is as much an organizational challenge as a technical one. Deloitte's Defense & Resilience practice helps organizations navigate the full journey: establishing business-led impact tolerances, assessing current capability against the ResOps framework, designing the cross-functional governance structures that sustain the discipline, and building the regulatory evidence and board-level reporting that modern compliance demands.

The most important work in ResOps cannot be delegated to IT. Defining what matters most – which services must survive, how much disruption is tolerable, and what good recovery looks like in business terms – requires genuine executive alignment. A risk leader may view one application as critical, while the CEO may see it differently. Getting to a unified, business-led answer to "what is our minimum viable company?" is the foundation on which everything else is built.

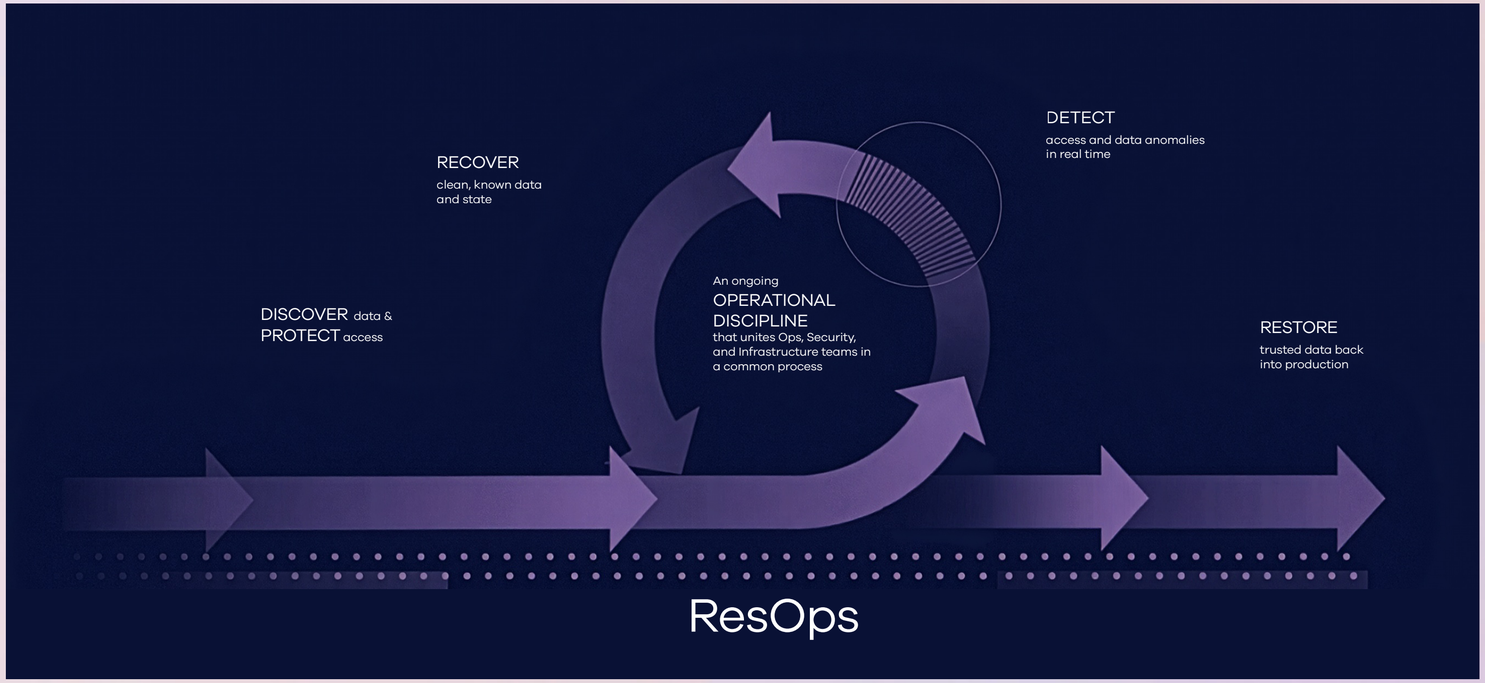
From there, Deloitte conducts a structured gap assessment mapped to the ResOps pillars and framework, defines the ResOps program enhancement roadmap, designs the ResOps Council structure and governance model, and helps organizations build audit-ready evidence that regulators, including under DORA, SEC disclosure rules, NIS2, and NIST CSF 2.0, increasingly require.

The most important work in ResOps cannot be delegated to IT.



Commvault + Deloitte.

How Commvault Enables ResOps



Recovery is only valuable if what you recover is clean. Commvault's Cleanroom Recovery capability restores systems into an isolated, verified-clean environment before reintroduction to production – helping reduce the risk of restoring malware or compromised configurations alongside legitimate data.

Immutable, air-gapped backups protect the recovery point itself. Anomaly detection and deep scan analytics continuously evaluate backup data for indicators of compromise, providing the ongoing validation signal that ResOps requires.

Commvault helps address the gap between theoretical and demonstrated recoverability through automated, continuous validation: testing that critical systems can be restored within defined impact tolerances, that recovery sequencing aligns to actual dependencies, and that backup integrity is confirmed. Results generate documented, audit-ready evidence that feeds directly into SRI dashboards and board-level reporting, helping transform validation from a calendar event into a continuous operational signal.

Underpinning both is unified visibility across data protection, identity resilience, and cyber recovery in a single platform. With credential abuse the most common breach vector[2], identity recovery must be as mature as data recovery. When data protection, identity resilience, and cyber recovery operate from shared telemetry, the continuous ResOps loop can be automated and sustained as a genuine operating model.

2. 2025 Data Breach Investigations Report, Verizon

Commvault + Deloitte.

Final thoughts

Having a recovery plan and being able to execute one are different things. Most organizations have invested in the former. ResOps is the operational discipline that closes the gap, building on the minimum viability foundation to make recoverability something the organization can demonstrate, govern, and improve continuously rather than periodically assert.

Commvault provides the technology platform (clean recovery, continuous validation, and unified resilience visibility) that makes ResOps operationally real. Deloitte provides the strategy, the program enhancement roadmap, operating model design, and industry-leading governance experience to make it organizationally sustainable.

Together, Commvault and Deloitte can help organizations confidently answer the question executives dread:
Yes, we can recover. We have proved it. And we can prove it again.