RESTORING WHAT MATTERS MOST

Minimum Viable Company

A Pragmatic Playbook for Enterprise Leaders

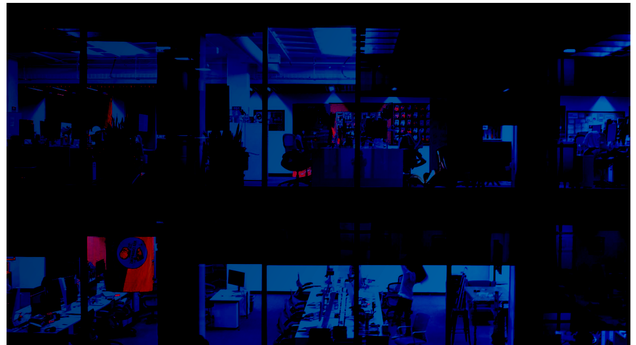
By **Bill O'Connell**, CSO, Commvault and **Sharon Chand**, Principal, Deloitte Defense & Resilience Leader

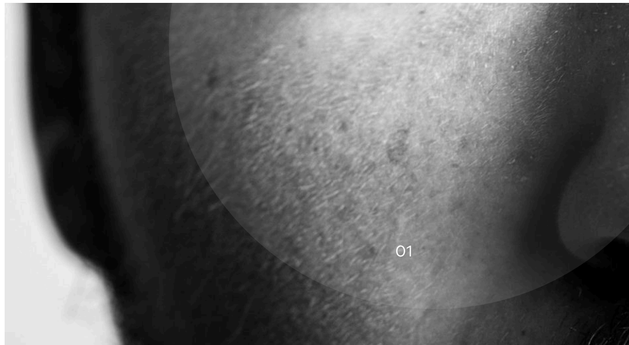
READIVERSE

Executive Summary

Commvault® + Deloitte.

Digital transformation is creating unprecedented opportunities for business innovation. This rapid digital advancement makes defining and protecting a company's minimum viable operations increasingly critical – so core business services remain resilient and operational, even as digital ecosystems grow more complex and interconnected. Agentic AI is poised to further accelerate this evolution, as organizations embrace increasingly sophisticated tools and workflows.





Executive Summary

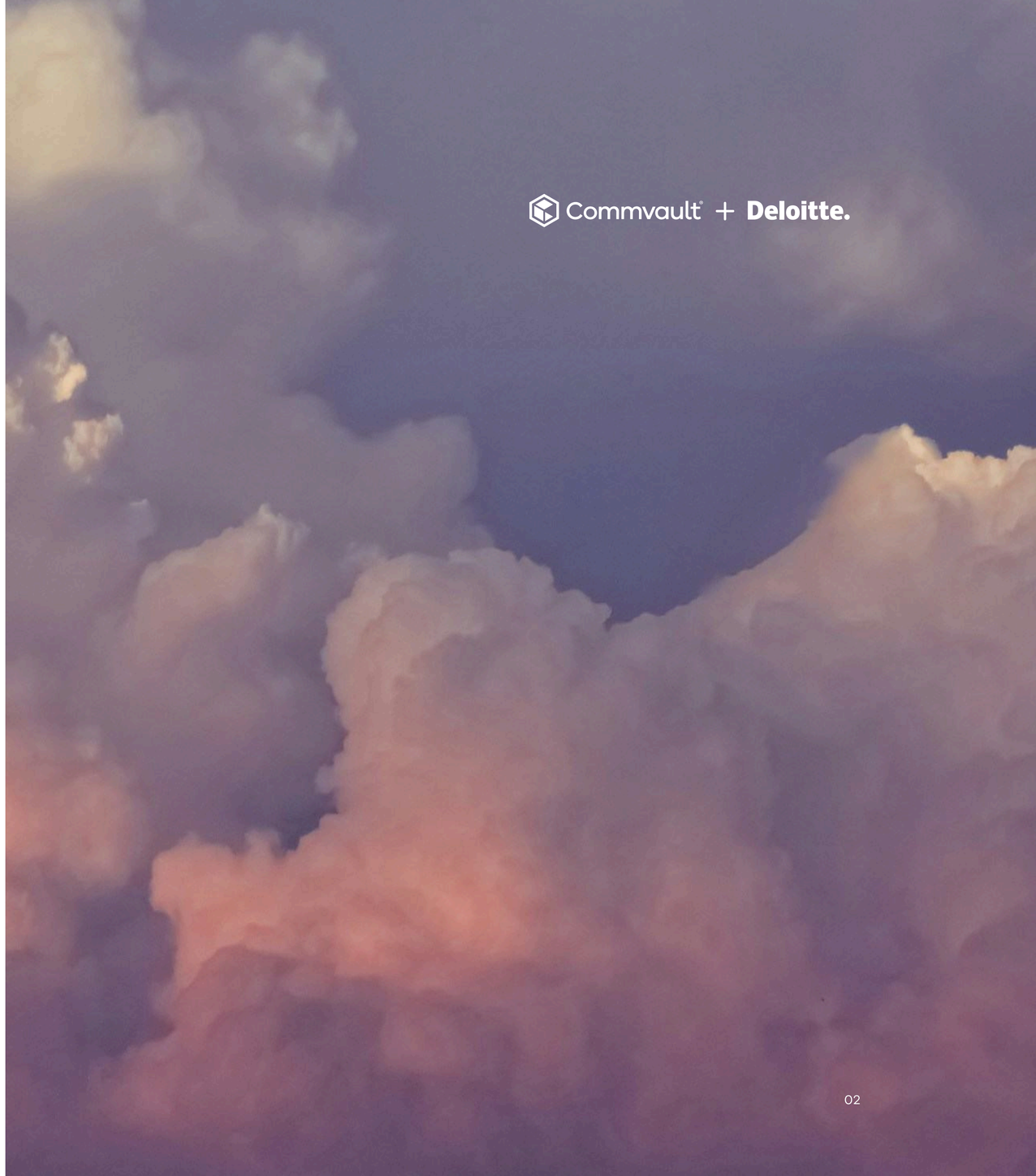
But what exactly is a minimum viable company (MVC)? Simply put, it represents the essential operational state of a business, allowing it to function and potentially grow, even if at a reduced capacity. In the context of cyber resilience, a minimum viability strategy pinpoints and safeguards the most critical resources, data, applications, and processes needed to restore vital operations during and after a cyberattack.

This paper explores **three essential components** of effective resilience planning:

We define the MVC framework, focusing on critical operations, applications, and data needed to maintain core functions during disruptions.

We highlight the importance of real-time and continuous testing to validate recovery capabilities and build organizational readiness.

We explore how organizations must integrate agentic AI into MVC planning, considering both potential vulnerabilities and resilience benefits.



Commvault + Deloitte.

Why is Minimum Viability important?

The financial impact of cyber threats is continuously rising, with every second of downtime causing **unprecedented costs** for businesses.

The average cost of downtime is estimated at

$14,056 PER MINUTE[1]

Data breaches are also on the rise, fueled by the exponential growth of AI-powered attacks, ransomware, and insider threats. Adopting an MVC approach can help to significantly reduce these potential financial impacts by prioritizing recovery of only the most essential business functions. By focusing resources on what truly matters for continuous business, organizations can decrease both recovery time and associated costs, while helping to prioritize restoration of revenue-generating operations.

Defining and implementing minimum viability is crucial, but it's not solely a technological pursuit. Effective recovery to minimum viable operations requires a comprehensive strategy that integrates people, processes, and technology. This holistic approach is essential for organizations across all sectors to maintain continuous business operations in the face of cyber adversity.

1. Enterprise Management Associates, "IT outages: 2024 costs and containment," Valerie O'Connell, Research Director, April 2024.

Minimum Viability Looks Different for Every Company

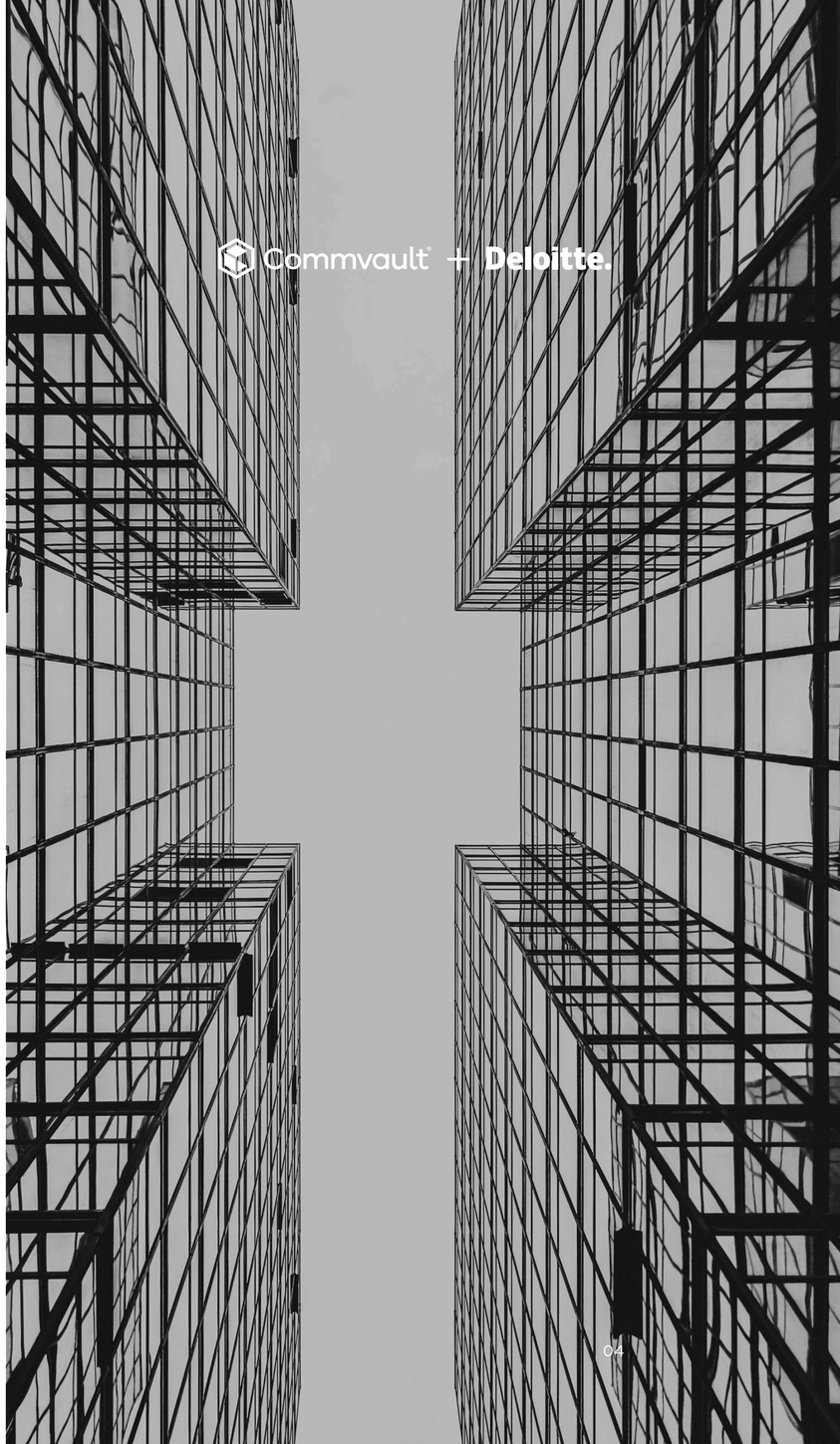
The specifics of an MVC vary depending on the nature of the business. In manufacturing, it might involve restoring essential production lines, including keycard access, machinery controls, and inventory. In healthcare, the priority would be patient care systems such as life support equipment, electronic health records, and pharmacy operations. Financial services companies would focus on securing transactions like fund transfers and fraud detection, while e-commerce businesses would need to keep their online store running, including the platform, inventory, and shipping.

Bridging the Gap: Aligning Business and IT for Minimum Viability

Traditionally, IT asset classification practices like server tiering and application mapping have been "bottom-up" exercises, focused on technical dependencies and infrastructure. However, the escalating threat of cyberattacks and the need for rapid recovery have fundamentally changed the landscape. Organizations now need a "top-down," business-aligned approach to define and achieve minimum viability.

This shift is crucial. While IT might categorize assets based on technical criticality, defining minimum viability calls for executive and business leader alignment on what truly constitutes "critical" for the organization to operate.

The question becomes: What are the essential business services that should be prioritized and restored to maintain core operations? This is where the difference lies. A risk/governance leader might view a certain application as critical, while the CEO and other business leaders might have other views of what is important. This highlights the need for a unified understanding of business priorities to effectively define minimum viability.



Commvault + Deloitte.

The advantages of this business-driven approach are clear:

Minimum viability gives urgency and importance to the decades-old practice of IT asset classification.

This perspective transforms traditional IT exercises into strategic business imperatives, keeping recovery efforts focused on restoring what truly matters most to the organization.

The Importance Server Tiering and Application Mapping Play in minimum viability

Understanding the interdependencies within their IT infrastructure and business processes is essential for organizations to effectively prioritize recovery efforts and facilitate continuous business. This is where server infrastructure tiering, application mapping, and observability come into play.

Business process analysis: Identifies critical business processes that support the operations fundamental to the company's business.

Server infrastructure tiering: Involves categorizing servers (including physical, virtual, cloud workload) based on their criticality to business operations. Tier 0 servers typically support mission-critical business processes and applications and require the fastest recovery times, while Tier 3 servers may support less-critical functions

Application mapping: Identifies the relationships between applications and the cloud services or infrastructure on which they rely. This focuses investments in resilience by connecting the end-to-end business services with the technology and third parties needed for minimum viability.

Observability: Implement processes and capabilities to improve recovery intelligence and monitoring of key data for critical functions, integrations, platform health, and recovery risks.

By incorporating business process analysis, server tiering, application mapping, and observability into their minimum viability planning, organizations can:

Maintain operational resilience: Enable critical services to continue operating even during disruptions, providing utility-like reliability that customers and regulators expect.

Implement degraded-state functionality: Design systems to gracefully reduce capabilities during incidents rather than failing completely, prioritizing continuity of essential customer-facing services.

Optimize resource allocation: Distribute resources effectively based on the criticality of servers and applications, maximizing operational continuity during challenging conditions.

Confirming minimum viability interdependencies through testing

Regular testing is a critical component of any robust minimum viability strategy. Thorough testing allows organizations to validate their recovery plans and assess the functionality of their essential systems.
By simulating various scenarios, organizations can:

Identify gaps and weaknesses in their recovery plans, such as missing dependencies or insufficient resources.

Enhance recovery processes to improve efficiency and effectiveness.

Build confidence in their ability to recover from a cyberattack and maintain business operations.

Importantly, testing can reveal hidden interdependencies that might not be apparent during planning. This proactive approach enables organizations to address potential issues and refine their minimum viability strategy, making them better prepared to face any disruption.

Commvault + Deloitte.

Testing at the Speed of Digital Innovation

Static recovery plans quickly become obsolete. True cyber resilience requires continuous validation to keep up with technological advancements. Organizations must shift from periodic exercises to ongoing testing frameworks that verify recovery capabilities as systems evolve. Effective testing uncovers hidden interdependencies and builds organizational muscle memory. Regular simulations, tabletop exercises, and cyber recovery drills provide teams with confidence in executing plans under pressure. This proactive approach keeps minimum viability strategies practical and aligned with current operations.

Agentic AI: the New Frontier in MVC planning

The rise of agentic AI – systems that autonomously pursue goals rather than simply respond to prompts – marks a significant shift requiring strategic resilience planning.

Defining the Agentic Challenge

Unlike generative AI that creates content based on patterns, agentic AI can independently plan, execute, and adapt. This shift introduces new complexities for MVC planning:

Expanded attack surface
Agentic AI interacting with critical applications can create new entry points for threats.

Dependency vulnerabilities
MVC strategies must account for AI-dependent workflows, which can become essential to core operations.

Rapid decision implementation
Agentic systems can execute decisions quickly without human oversight, potentially amplifying the impact of compromised systems or faulty logic.

Incorporating Agentic AI in your MVC Framework

The same autonomous capabilities that create new risks also offer significant opportunities for enhancing resilience.

Proactive defense: Agentic systems can autonomously take protective actions, like snapshotting virtual machines, verifying backups, and isolating suspicious endpoints, to reduce attack impact.

Intelligent recovery: Agentic AI can analyze attack scope, identify optimal recovery points, orchestrate restores, validate data, and generate reports to prioritize critical systems.

Dynamic orchestration: Agentic systems can coordinate complex workflows across hybrid environments to restore critical systems to their pre-attack state, focusing on essential components.

Practical Steps for Integrating Agentic AI into MVC Planning

Organizations seeking to leverage agentic AI for enhanced resilience should consider several actions, including:

Identify AI-dependent critical paths: Document which core business functions now rely on AI systems and include these in MVC mapping.

Establish agent guardrails: Define clear boundaries for autonomous agent actions, especially during crisis scenarios.

Deploy recovery-focused agents: Implement specialized agents programmed to prioritize MVC components in recovery scenarios.

Maintain human oversight: Confirm that critical decision points include human verification while leveraging machine speed for implementation.

Test agent-led recovery: Incorporate agentic AI recovery scenarios in regular testing exercises to validate effectiveness and build organizational confidence.

Commvault's Part in MVC

Commvault is a leading provider of cyber resilience solutions, empowering organizations to prepare for, withstand, and recover from cyberattacks. Commvault's comprehensive suite of tools and services helps organizations establish and maintain their minimum viability. These solutions go beyond simply backing up data, focusing on proactive defense, rapid clean recovery, and continuous business operations.

While Commvault provides powerful tools and services to support recovery to minimum viability, it's essential to recognize that defining the specific components of your organization's minimum viability is an internal process. No one understands your critical operations better than your own personnel. Determining which applications, data, and processes are essential for core operations requires internal business analysis, executive alignment, and a robust incident response plan. Ultimately, this involves identifying what matters most for your organization.

Key offerings include:

Recovery of Critical Data

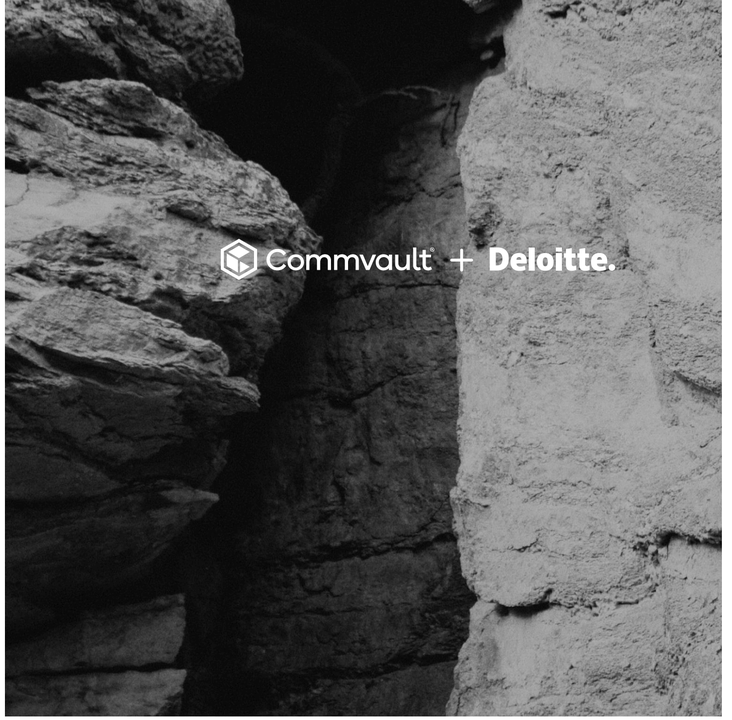
Commvault provides comprehensive data protection, cloud infrastructure as-a-service, clean point recovery, and the ability to isolate bad copies, enabling the recovery of critical data.

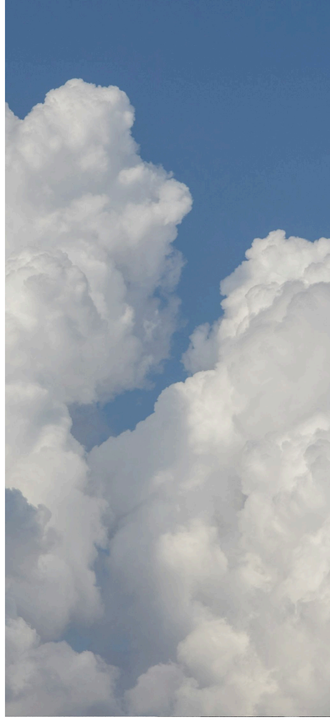
Data Security

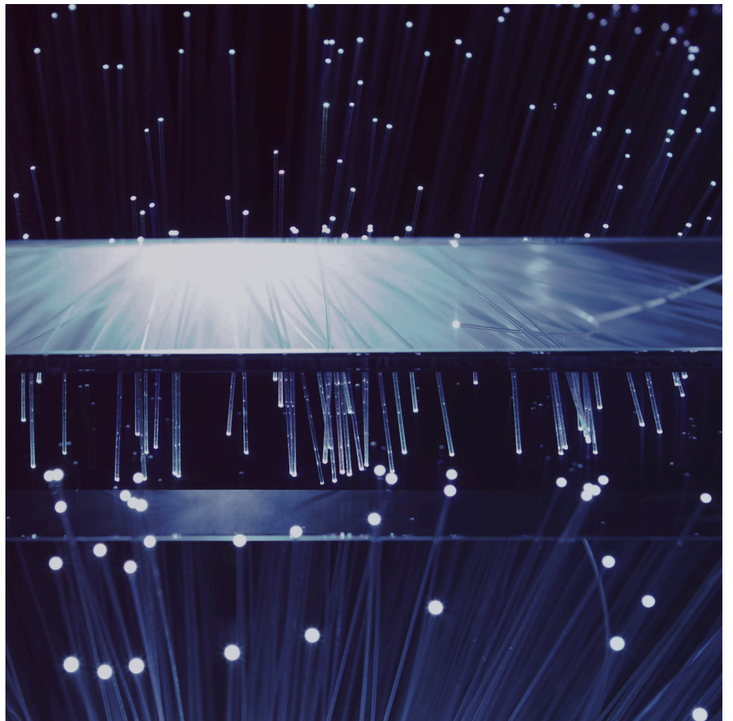
Commvault offers anomaly and threat detection, integration with third-party security tools, data access patterns, and deep scan analytics to enhance data security.

Secure and Isolated Recovery Environment

Commvault provides a cleanroom recovery environment, immutable and indelible air-gapped backups, secure access controls, and pave/repave capabilities to enable a secure and isolated recovery process to a trusted state.







Commvault + Deloitte.

Deloitte's Part in MVC

Deloitte is a global leader for cyber professional services. Deloitte's Cyber Risk Services practice helps organizations become more trustworthy, resilient, and secure through proactive management of cyber risks.

Deloitte assists organizations in enhancing their resilience programs to be better prepared for a cyber incident, including end-to-end cyber readiness, response, and recovery before, during, and after a cyber incident; and span across the following services areas:

Resilience Strategy

Resilience Strategy prepares and designs capabilities and processes to help organizations to effectively anticipate, respond to, and recover from disruptions and helps companies define their MVC by identifying and prioritizing critical business processes and supporting applications and infrastructure.

Business Resilience

Build end-to-end resilience into critical operations so you can more effectively protect your organization against significant disruptions.

Technical Resilience

Through innovative architecture designs and integrated technologies, Technical Resilience helps organizations shift the paradigm away from reactive recovery
measures toward a more proactive resilience-centered approach.

Cyber and Data Resilience

Improve your organization's resilience against a wide range of data disruption scenarios, including destructive cyberattacks and data breaches.

Resilience-as-a-Service

Deloitte offers a broad suite of managed services, including functional testing and continuous monitoring,
built upon the client's existing technology foundation so organizations can focus on what matters most.

Commvault + Deloitte.

Final thoughts

In the face of relentless cyber threats, a **well-defined minimum viability strategy is paramount.** This strategy necessitates a holistic approach that encompasses response plans, processes, and rigorous testing. By prioritizing critical resources, data, and applications, businesses can bolster their resilience and sustain essential operations amidst severe cyber disruptions.

Commvault's advanced tools and services empower organizations to establish, maintain, and swiftly recover their minimum viability, effectively navigating the ever-evolving cyber threat landscape. Deloitte's extensive expertise in resilience programs and operations helps clients further enhance their defense and recovery capabilities.

Together, Deloitte and Commvault can assist clients to enhance their full cyber defense and resilience programs, integrating people, processes, and technology.

Minimum viability extends beyond mere recovery; it enables organizations to continue to meet customer needs even in the face of adversity. Achieving this requires robust technology, a clear understanding of core functions, and an unwavering commitment to continuous preparedness.