Grant Thornton

Modern Digital Resiliency

A practical framework to help improve business resiliency in ever-changing times

An Executive Guide by Grant Thornton Digital

Executive Summary

The business landscape of 2025 presents unprecedented challenges for leaders. Digital transformation has fundamentally altered how organisations operate, creating both extraordinary opportunities and complex vulnerabilities.

Organisations today depend on interconnected systems spanning multiple cloud platforms, SaaS applications and hybrid infrastructures that extend far beyond traditional corporate boundaries.

The statistics reveal the stark reality of modern operations:

- Cloud computing market reached $805 billion in 2024, expected to double by 2028
- Cyber-attacks and data extortion account for 32% of all reported security incidents
- Average cost of unplanned downtime: $14,056 per minute per organisation
- 74% of enterprises don't utilise half of known resilience best practices

Modern organisations face converging threats that traditional business continuity approaches cannot address. Sophisticated ransomware groups are well organised and target critical infrastructure with precision-engineered attacks, while regulatory frameworks like the Digital Operational Resilience Act (DORA) demand higher standards.

The challenge extends beyond technology to encompass financial sustainability, digitally-savvy governance, operational excellence and optimised resilience ROI.

Assumptions around data availability and data protection can result in complacency. At the same time, organisations struggle with unpredictable cloud costs and complex multi-cloud environments.

Risk management processes remain largely manual and reactive, while business leaders recognise that resilient cultures drive higher productivity.

These issues are relevant to an organisation, but also to the leaders in those organisations. And those organisations can be of any size, in any industry – with cloud tools and applications now utilised by most organisations, everyone needs to consider how they can become more resilient.

The leading organisations thrive through systematic preparation. They've moved beyond reactive approaches to build comprehensive resilience frameworks that transform operational capability and future readiness.

For organisations to achieve sustainable success in the future, they need to work towards an end state that will not only serve their needs today – but ensure the they set themselves up to thrive in the future.

Modern Digital Resiliency is a framework that supports the needs of all leaders, delivering a pragmatic, visible and adaptive approach to helping ensure organisations are ready for future change.

Modern Digital Resiliency

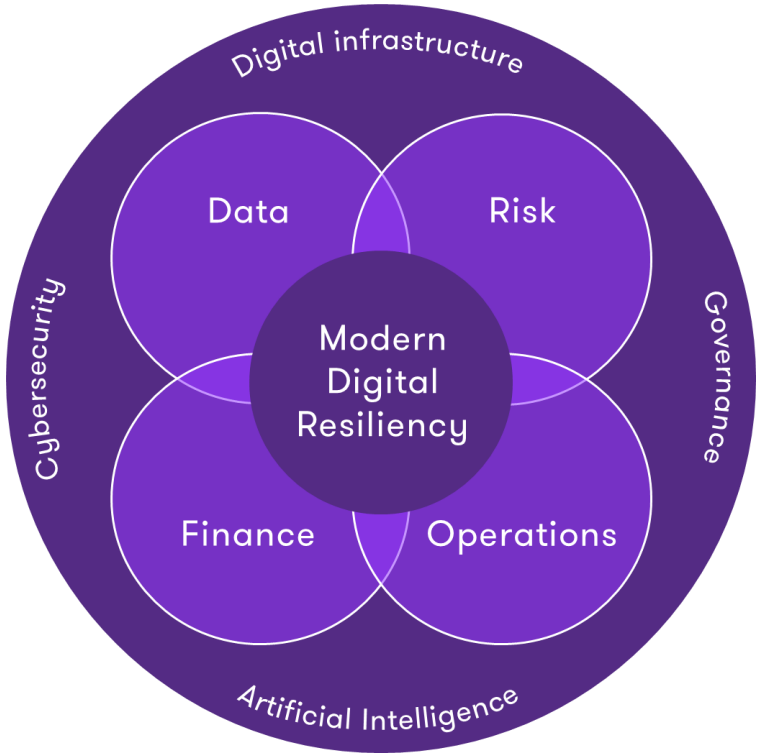
Despite significant investments in technology and security, most organisations operate with a dangerous confidence gap between perceived and actual resilience capabilities.

Research shows that one in two organisations globally lack comprehensive business continuity plans, while at the same time they also consistently overestimate their preparedness levels.

Traditional “business continuity” approaches that focus primarily on data backup and disaster recovery have proven inadequate for today's complex operational environment. Modern Digital Resiliency (MDR) requires a holistic approach addressing the entire ecosystem of capabilities that enable business continuity across all operational dimensions.

Modern Digital Resiliency establishes the baseline operational preparedness every organisation needs to thrive in an increasingly volatile digital landscape. This framework rests on four interconnected domains:

- **Modern Data Protection and Recovery** – Comprehensive data availability through modern backups supporting rapid recovery
- **RiskOps/CtrlOps** – Proactive risk identification and automated governance frameworks
- **FinOps** – Financial optimisation and cost management for sustainable business operations
- **Cloud InfraOps** – Scalable, reliable infrastructure support to ensure ongoing management and optimisation



Each domain addresses critical aspects of organisational resilience, but their true power emerges when they function as an integrated ecosystem, underpinned and accelerated by digital infrastructure, cybersecurity, governance and artificial intelligence (AI).

Implementing a MDR programme can help drive a range of tangible and intangible outcomes: faster recovery speed, less downtime, less data loss, and higher revenue growth. With practical approaches and pragmatic actions, MDR provides guidance for any organisation to become future ready.

Modern Data Protection and Recovery

Data is the lifeblood of modern organisations, underpinning all our core systems. Yet data protection strategies often fail to keep pace with data sprawl across on-premises servers, public clouds, SaaS applications and edge devices.

Modern Data Protection and Recovery encompasses a comprehensive approach ensuring not just data preservation, but rapid business restoration across all critical environments.

Organisations frequently discover that perceived data protection contains critical gaps that become apparent only during crisis situations. SaaS applications remain unprotected, cloud workloads receive inconsistent coverage, and backup systems themselves become attack targets.

Modern data protection addresses these challenges through:

- **Multi-platform coverage** across on-premises, cloud platforms, and SaaS applications
- **Immutable storage protection** preventing ransomware encryption and insider threats
- **Automated verification** continuously testing backup integrity without human intervention
- **Cross-platform restoration** enabling recovery to different environments than origin points

Data recovery is equally critical; data protection without rapid restoration provides little business value. Modern recovery approaches enable granular restoration from individual files to entire data centres, with recovery times measured in minutes rather than hours when planned and implemented well. Automated failover systems detect failures and initiate recovery without waiting for human intervention.

Many organisations have not fully appreciated the nuances of data protection in the emergent world of cloud's "shared responsibility" model and the utilisation of software services, where the reality of how and where data is protected is often assumed, creating grey areas of responsibility.

And as data is increasingly used to power customer interactions, reliance on it grows – particularly as AI increasingly plays a part in business operations, adding a new dimension to data availability and access.

Organisations who are concerned about the resiliency of their data should look at options to further protect themselves.

RiskOps and CtrlOps

The transformation from reactive risk management to proactive resilience represents a key shift in how modern organisations approach operational risk and governance.

Traditional risk management operates through periodic cycles of quarterly assessments and reactive incident response that proves inadequate for today's dynamic threat landscape. For most organisations, risks are assessed, mitigations are identified, but often there is minimal ongoing management.

RiskOps and CtrlOps apply DevOps principles to risk management and governance, creating continuous, automated processes that identify, assess and mitigate risks before they manifest as business disruptions.

Organisations embracing RiskOps move beyond static risk registers to dynamic, real-time risk intelligence aligned with operational decision-making. Key capabilities include:

- **Continuous monitoring of risk indicators** across systems, processes, and third-party relationships
- **Predictive analytics** using historical data and machine learning to identify emerging risks
- **Automated escalation** routing risk information to stakeholders based on severity and impact
- **Policy-as-code implementation** translating organisational policies into automated controls

CtrlOps provides observability for the risk management function, providing the requisite control testing functions to ensure consistency, quality and helping better manage the rest of the risk management framework.

As regulatory deadlines become increasingly strict and companies face accountability for an evolving set of regulations and changing environments, manual compliance processes cannot scale to meet demands.

The business benefits of CtrlOps can prove substantial and measurable. Research indicates organisations typically report significant reductions in audit preparation time as evidence collection becomes automated and continuous.

The opportunity of an automated process is compelling, though: Early warning systems help organisations address issues before they escalate into crises, while automated governance demonstrates commitment to stakeholders and regulators, allowing organisations to better understand and respond to ever-changing situations.

Financial Operations (FinOps)

The discipline of FinOps has emerged as a critical pillar of organisational resilience as cloud computing costs become an increasingly significant portion of operational expenses.

Organisations frequently struggle with cloud cost unpredictability that undermines budgeting processes and strategic planning, or results in unwanted surprises when cloud costs balloon.

Project, development, digital and IT teams spin up resources without always considering financial implications, while finance departments attempt to budget for inherently variable services.

FinOps has emerged a new services capability designed to help organisations better manage these costs.

Effective FinOps implementation progresses through three distinct maturity phases:

1. **Visibility and Allocation** – Real-time spending analytics, accurate cost attribution, and trend analysis
2. **Optimisation and Control** – Resource rightsizing, strategic commitment management, and automated optimisation
3. **Strategic Alignment** – Business value mapping, innovation enablement, and predictive planning integration

In addition to traditional cloud spend, modern FinOps must also address the impending costs of artificial intelligence and machine learning, as companies invested in AI can see significant, unexpected cloud bill impacts.

Sustainability integration also becomes important as organisations balance the resilience, cost and environmental impact considerations of using cloud. Organisations can progressively introduce FinOps into their operations and can establish FinOps functions that are proportional to the organisation's cloud and management needs and overall maturity.

By better managing cloud costs, organisations achieve greater levels of financial resiliency, with savings used to sustain the business or to reinvest in other areas.

Cloud InfraOps

The complexity of modern cloud operations has created a critical skills gap challenging organisations across industries.

Managing sophisticated multi-cloud environments requires expertise across multiple domains including multi-cloud architecture, DevOps automation, security and compliance, cost optimisation, and round the clock support.

Cloud InfraOps bridges the gap between organisational needs and realistic internal capabilities. Professional teams deliver comprehensive operational excellence through:

- **24/7 monitoring and response detecting** and addressing issues before business impact
- **Proactive maintenance** including optimisation, patching, and capacity planning
- **Performance optimisation** through continuous infrastructure tuning for cost, performance, and security
- **Strategic initiatives** encompassing capacity planning, architecture reviews, and technology road mapping

The strategic benefits extend beyond operational tasks to provide access to certified professionals across major cloud platforms, expertise that individual organisations cannot economically maintain. Best practice implementation applies proven methodologies, while continuous optimisation ensures infrastructure evolution matches business requirements.

The business case encompasses multiple value dimensions beyond simple cost considerations. Risk mitigation through security monitoring, compliance assurance, and business continuity capabilities provides quantifiable value.

Avoided downtime becomes particularly valuable given that unplanned downtime costs for an organisation can be significant.

Clear demarcations can be put in place to enable internal teams to concentrate on business-differentiating activities rather than operational maintenance, while a Cloud InfraOps provider can utilise skills and third-party tools to help provide the visibility and control needed to manage and optimise often mission critical systems.

Digital Infrastructure: The foundation of resilience

Modern organisations rely on a complex mesh of interconnected applications, platforms, and networks to operate effectively. As businesses become ever more dependent on digital systems, resilience increasingly relies on the strength of their underlying infrastructure.

A reliable, scalable, and secure digital foundation ensures that critical applications and data can be delivered consistently, even in the face of unexpected disruption.

Today, infrastructure is no longer confined to on-premises data centres. Most organisations operate hybrid or multi-cloud environments where compute, storage, and networking resources are distributed across multiple providers and regions. This brings unparalleled agility and scalability, but also new dependencies and risks.

Resilient digital infrastructure involves:

- **High availability architecture:** Redundant systems, failover capabilities, and globally distributed resources minimise downtime
- **Elastic scalability:** The ability to expand or contract resources dynamically to meet unexpected demand spikes or crises
- **Built-in security and compliance:** Infrastructure designed with layered defences, encryption, and alignment to evolving regulatory frameworks
- **Automated observability and optimisation:** Real-time monitoring, patching and self-healing capabilities to maintain performance and control costs

By focusing on these principles, organisations can ensure the platforms underpinning their operations are ready to support critical applications, protect sensitive data, and maintain continuity regardless of circumstances.

Importantly, infrastructure resilience is not just a technology issue; it is a business imperative. In a digital economy, the infrastructure layer directly impacts customer experience, revenue generation and brand reputation.

As with all areas of Modern Digital Resilience, organisations should approach digital infrastructure with clear strategies, defined operational playbooks, and access to the right expertise. Leveraging leading cloud providers, best-in-class tools, and proven methodologies enables them to build an environment that is not only stable today but adaptable to future challenges.

Amazon Web Services (AWS) is a recognised leader in cloud infrastructure, offering unmatched global scale, reliability, and security.

Partnering with AWS allows organisations to reduce risk, accelerate innovation, and confidently deliver seamless experiences to their customers – even in times of disruption.

With its new data centre region in New Zealand, AWS sets a new standard in high-calibre digital resilience for New Zealand organisations.

Integration and implementation

The true power of Modern Digital Resiliency emerges when all four domains function as an integrated ecosystem rather than isolated initiatives.

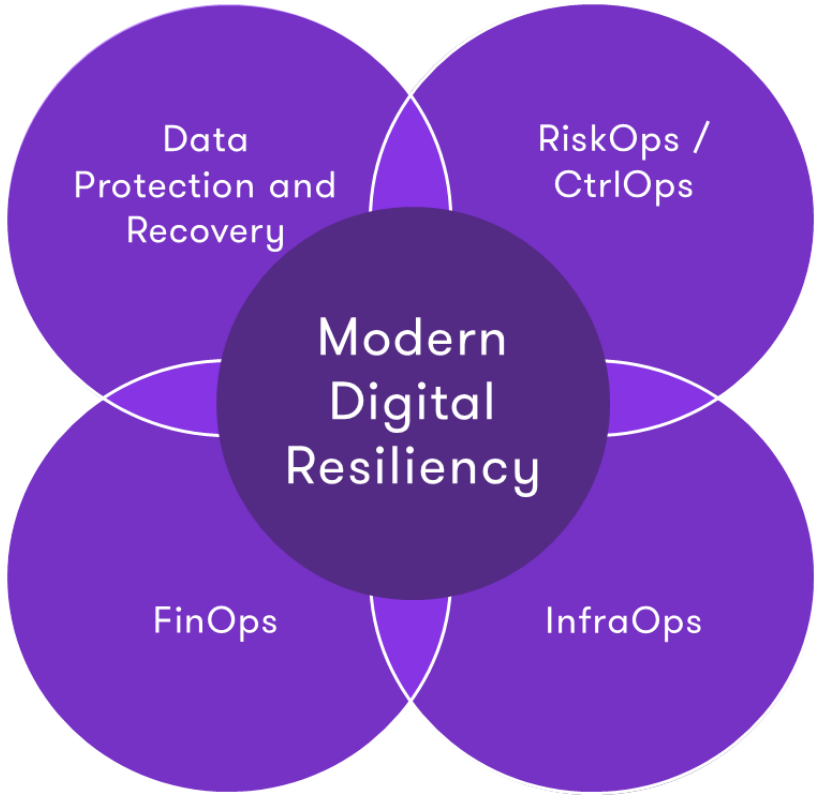
But while integration can create powerful synergies organisations can progressively adopt capabilities based on their priorities, capabilities and investment – MDR doesn't have to be an all-or-nothing initiative.

Organisations wanting to embrace Modern Digital Resiliency can start with any of the four domains and can choose when to progress to other areas.

All domains will, in time, deliver a cumulative level of resiliency, however for most organisations the important step is to get started. Whether you're looking at implementing a backup solution, or transforming into a fully-resilient business, the Modern Digital Resiliency framework is here to help.

Modern data protection generates operational intelligence including backup success rates, recovery test results, and security events that, when integrated with RiskOps platforms, and CtrlOps toolsets, can automatically update risk scores and trigger appropriate responses. Similarly, combining Cloud InfraOps with sophisticated cost optimisation creates feedback loops where the cloud operations teams provide operational discipline to implement FinOps recommendations.

Similarly, FinOps provides financial intelligence to guide infrastructure decisions, based on actual and forecasted spend.



Considered separately or as a set, the Modern Digital Resiliency framework provides flexibility when it comes to integration and implementation and can be aligned with your strategic and operational priorities.

Measuring success and ROI

Organisations implementing comprehensive Modern Digital Resilience frameworks consistently demonstrate measurable improvements across operational, financial and strategic dimensions that help to justify investment and can be used to guide optimisation efforts.

Operational metrics show dramatic improvements in key performance indicators directly impacting business continuity and customer satisfaction:

- **Recovery time improvements** – Faster mean time to recovery
- **Downtime reduction** – Less disruption duration
- **Data loss prevention** – Less data loss during incidents
- **Incident response** – Faster detection and containment capabilities

Financial impact demonstrates clear return on investment through multiple channels. Improved operational stability can result in revenue growth rates as organisations maintain market presence during disruptions affecting competitors.

Cost optimisation delivers significant reductions in cloud spending and operational overhead, while risk mitigation provides measurable value through lower insurance premiums and reduced regulatory fines – not to mention the reputational benefits associated with business resiliency.

Strategic advantages become increasingly apparent as organisations develop competitive differentiation through superior reliability compared to industry peers. Market responsiveness improves through faster deployment of new capabilities, while stakeholder confidence increases through demonstrated resilience capabilities. Regulatory compliance becomes simplified through automated audit processes and reduced compliance costs.

Regardless of how success is measured, implementing Modern Digital Resilience will deliver many direct and indirect benefits.

The Resiliency Imperative

The business imperative for Modern Digital Resiliency has never been more urgent or clear.

Organisations operating in 2025 face unprecedented challenges from sophisticated threat actors, geopolitical changes, complex technological dependencies, stringent regulatory requirements, and stakeholder expectations for operational excellence.

The consequences of inadequate preparation can be severe:

- **90% of businesses fail within a year** if unable to recover within five days after disaster
- **59% of organisations experienced ransomware** attacks in 2024
- **Global average data breach costs** reached $4.88 million
- **Average unplanned downtime costs** $14,056 per minute

Yet research demonstrates the clear path forward for organisations willing to invest in modern resilience capabilities.

Top performers achieve superior outcomes across all critical dimensions while building sustainable competitive advantages through superior reliability, faster innovation, and strategic resource utilisation.

The four domains of Modern Digital Resilience provide a proven framework addressing the full spectrum of modern operational challenges. Organisations can choose to embrace all four domains or can be selective, basing their approach on priorities, capacity and direction.

The question facing every organisation isn't whether to implement Modern Digital Resilience, but how quickly these critical capabilities can be established. Every day without adequate digital resilience increases organisational risk, increases cost, and creates competitive vulnerability, while readiness creates sustainable competitive advantages.

Your customers, employees, and stakeholders depend on your organisation's ability to maintain operations when disruptions occur.

Modern Digital Resilience provides the framework, guidance, and proven approach to ensure your organisation not only survives the next inevitable crisis but emerges stronger and more competitive than before.

Explore how your organisation can adopt Modern Digital Resilience.

Visit www.grantthornton.co.nz/services/modern-digital-resiliency/