Modernising operational resilience programs:

Why the time is now

Building resilience as a strategic capability — powered by program maturity, connected data, and technology enablement.

A market at an inflection point

Operational resilience has evolved from a compliance-driven expectation to a strategic capability critical to enabling business continuity and fostering trust. Organisations today should anticipate, withstand, and recover from disruptions not simply to meet regulatory obligations, but to safeguard brand, performance, and customer confidence in a hyperconnected world prone to disruption.

Yet most programs remain fragmented:

- Disparate ownership between risk, operations, IT, and security functions.
- Manual, disconnected processes for testing, reporting, and dependency mapping.
- Outdated recovery plans unable to keep pace with digital transformation.
- Limited visibility across critical services, vendors, and infrastructure dependencies.

As digital interdependencies grow spanning cloud, AI, and third-party ecosystems, organisations are shifting from response and recovery to continuous, connected resilience.

Regulators and standard-setters are also aligning around this shift. The recently updated NIST Cybersecurity Framework (CSF) 2.0 expands beyond cybersecurity to include governance, risk, and resilience, reinforcing the need for unified oversight across technology, operations, and supply chain. Similarly, DORA, UK PRA, MAS, and OSFI E-21 guidelines are converging on shared principles of end-to-end resilience.

The question is no longer “Can we recover?” it’s “How quickly can we adapt without losing customer trust or operational continuity?”

Program first: Building the foundation for operational resilience

PwC views operational resilience as a maturity journey, not a static project. Each organisation progresses through distinct stages evolving from isolated recovery plans to integrated, enterprise-wide resilience programs.

The operational resilience journey

1

Create the mandate and prioritise:

Define vision, leadership commitment, and cross-functional alignment. Conduct a maturity baseline, identify critical services, and establish governance and funding for resilience initiatives.

2

Build and understand:

Formalise governance and roles. Map critical operations and dependencies across business, data, people, applications/infrastructure, facilities, and third parties

3

Embed, test, and enhance:

Execute Business Impact Analysis (BIA), set impact tolerances, and conduct recovery testing and simulations. Establish metrics and KRIs that measure resilience performance, demonstrate reduction in risk, and drive improvement.

4

Respond and Improve:

Develop continuous learning and feedback loops with regular testing, reporting, and adaptive governance. Mature toward automated testing, real-time monitoring, and predictive insights.

This programmatic approach transforms resilience from a static compliance function to a living capability that adapts to business change.

Program governance and operating model

Modern resilience programs are governed at the enterprise level, integrating business, risk, and technology. Key success factors include:

Unified governance:

A cross-functional model connecting risk, operations, technology, and compliance.

Defined ownership:

Clear accountability for critical services and dependencies.

Measurement frameworks:

KPIs and KRIs that track performance against impact tolerances.

Embedded alignment:

Integration with frameworks such as NIST CSF 2.0, which brings resilience into the broader governance and cybersecurity ecosystem.

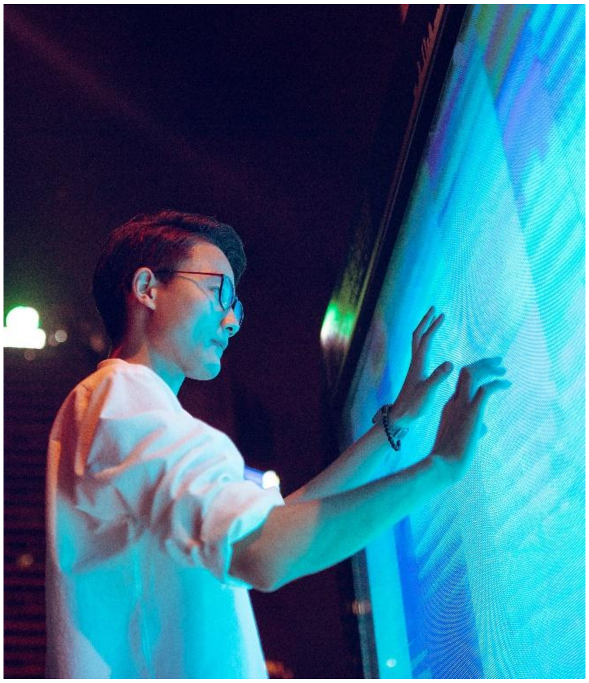
Organisations aligning with frameworks like NIST CSF 2.0 are redefining resilience as a data-driven, enterprise-wide discipline.

Technology-enabled resilience

Technology is not the starting point. It's the accelerator that enables scale, insight, and automation. When grounded in the right governance and data, technology becomes the connective fabric of resilience.

Core capabilities of modern resilience platforms:

- End-to-end visibility: Map and manage business services, assets, and dependencies in one unified system of record.
- Automated testing and scenario planning: Simulate disruptions and stress-test operations against impact tolerances.
- Integrated data model: Connect risk, continuity, IT operations, and third-party data for unified decision-making.
- Real-time monitoring: Enable proactive issue detection and rapid response.
- Intelligent workflows: Automate select response, communication, and escalation procedures and BAU activities such as refreshing BIAs.
- Analytics and reporting: Deliver real-time resilience dashboards for executives and boards.



Technology connects the dots but only a strong program can make those connections meaningful.

Emerging practices shaping the future of resilience

Resilience is evolving from recovery to anticipation. Organisations at the forefront of resilience are adopting forward-looking practices that help blend technology, data, and intelligence:

Resilience by design

Embedding continuity and risk principles directly into system and process architecture.

AI-enabled risk sensing:

Using AI to identify and predict early indicators of operational disruption.

Digital twin simulation:

Testing resilience scenarios virtually to model dependencies and outcomes.

Data-driven decisioning:

Integrating resilience metrics into enterprise performance dashboards.

Continuous validation:

Leveraging automation to test readiness and track real-time performance.

Industry nuances we're seeing

- **Financial Services:** Driven by US, EU PRA, and OSFI requirements, focusing on enhancing operational resilience.
- **Energy and Utilities:** Prioritising operational safety, infrastructure continuity, and renewable transition with limited investment capacity, modernisation should prove ROI.
- **Healthcare and Life Sciences:** Focused on safeguarding patient care, clinical operations, and supply chains amid tightening data integrity and resilience requirements.
- **Technology, Media and Telecommunications:** Complex global operations with fragmented tools across business units; many are now modernising to unify platforms and governance.
- **Manufacturing and Supply Chain:** Building supply chain resilience and integrating cyber-physical risk management into operational continuity programs.

How PwC can help

PwC helps organisations modernise, scale, and future-proof their operational resilience programs by bringing together strategy, governance, and technology enablement.

- **Program strategy and roadmap:** Define vision, scope, maturity path, and measurable outcomes.
- **Business case and ROI:** Identify both quantitative and qualitative value, including efficiency gains, risk reduction, and performance improvements.
- **Governance and operating model:** Align roles, accountability, and decision-making across business, risk, and technology.
- **Service and dependency mapping:** Create visibility into critical services, assets, and relationships across people, data, systems, and third parties.
- **Technology enablement:** Implement and enhance resilience platforms to automate workflows, testing, and reporting.
- **Testing and continuous improvement:** Conduct simulations, monitor performance, and refine capabilities through metrics and feedback.
- **Managed services:** Operate and sustain resilience programs and supporting technology to maintain maturity.

The bigger picture

Operational resilience is central to organisational resilience connecting people, processes, data, and technology into a single framework of trust.

Those who act now will not only withstand disruption they will likely outperform competitors by recovering faster, safeguarding value, and earning trust.

Resilience is no longer about bouncing back it's about moving forward with confidence.

PwC perspectives on operational resilience

The following examples highlight how PwC sees AI being applied across governance, risk, and compliance use cases. Read more at **pwc.com/crisis-solutions**

Theme	What leading organisations are doing
Program Integration	Aligning business continuity, crisis management, and IT recovery into one framework with unified governance.
Data and Technology Enablement	Implementing resilience platforms to automate testing, integrate data, and visualise dependencies.
Resilience Metrics and Reporting	Establishing quantifiable measures of recovery time, impact tolerance, and operational continuity.
Alignment with Global Frameworks (NIST, DORA, ISO)	Embedding NIST CSF 2.0 and related standards into resilience governance to unify cybersecurity, IT, and operational oversight.
Leadership and Culture	Shifting accountability from risk teams to business owners through cross-functional governance and culture change.

About PwC's Global Centre for Crisis Resilience

We've helped thousands of organisations globally as their trusted business advisor before, during and after crisis: from building robust enterprise resilience capabilities to strategically navigating disruption as it happens. We convene the right specialists across the globe in times of crisis within a matter of hours, helping organisations prepare for and recover from business disruption—and build resilience for what's next.

We bring the **right professionals** to you, **quickly**

We enable you to **continue to run the business**

We identify **priorities** while not losing sight of the **bigger picture**

We share **insights** specific to your industry, region, and disruption type

★ Presence of Territory Crisis & Resilience Leads

725 **Clients** served (FY24)

1,500 + **Crisis & resilience** professionals

Prepare

- Resilience maturity assessments
- Enterprise resilience
- program builds and enhancements
- Exercises and simulations
- Crisis and resilience training
- Technology enablement of program

Respond

- Strategy and governance
- Integrated response management and crisis coordination
- Operational response and fact finding
- Legal and regulatory support

Emerge stronger

- Recovery strategy and "looking around the corner"
- Operational remediation and financial restructuring
- Lessons learned and integration
- Enhanced organisational resilience

Contact us

David Stainback

Global Crisis & Resilience Co-Leader,
PwC United States
david.stainback@pwc.com

Bobbie Ramsden-Knowles

Global Crisis & Resilience Co-Leader,
PwC United Kingdom
roberta.ramsden-knowles@pwc.com

© 2025 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.