Connecting risk and resilience to protect what matters most

The resilience lens: a fresh perspective on risk management in industries beyond Financial Services

June 2025

pwc

Reframe: Change the way we see risk and resilience

We live in a world where disruption is commonplace. Resilience is no longer a 'nice-to-have'; it is a strategic imperative. This landscape, coupled with a number of resilience-focused regulatory initiatives – such as the EU Digital Operational Resilience Act, Telecommunications Security Act, Critical Third Parties regime, and the EU Critical Entities Resilience Directive – has led organisations across sectors to strengthen their resilience.

There has also been renewed focus on risk and resilience in the Financial Reporting Council's (FRC) UK Corporate Governance Code, including a requirement for organisations to declare the effectiveness of material controls – potentially covering those that support resilience to risks threatening the business model, solvency, or liquidity.

The growing focus on disruption has shifted attention away from business-as-usual (BAU) risk management, despite the close connection between risk and resilience. Now is the time to identify overlaps and use them to strengthen the resilience of critical services and/or products.

The rapid development of resilience strategies offers a chance to align risk and resilience with broader business goals.

Developing an integrated view of risk and resilience

Achieving integration means establishing both **preventative controls**, to minimise the likelihood of severe but plausible scenarios from materialising, and the building of '**resilience by design**'. This will enable firms to better anticipate and mitigate cascading contagion events in their environment.

Firms must assess how disruptions impact risks and controls, identifying where BAU controls may need to be **substituted** to maintain critical services. This requires close collaboration between resilience and risk teams to agree on substitutions and monitor associated risks.

Now more than ever, resilience and risk leaders – backed by executive support – must focus on a strategic vision for operational resilience. This involves **not only meeting regulatory requirements but also implementing the necessary changes to sustain resilience in the long term.**

Reassessing first and second line expectations is essential to fully integrate risk and resilience, turning them from compliance tasks into strategic enablers.

This paper explores these connections and outlines strategies for embedding risk and resilience into the broader business framework. **It addresses two key questions:**

How does risk and resilience work in tandem within an organisation to prevent disruptions and enhance response and recovery strategies?

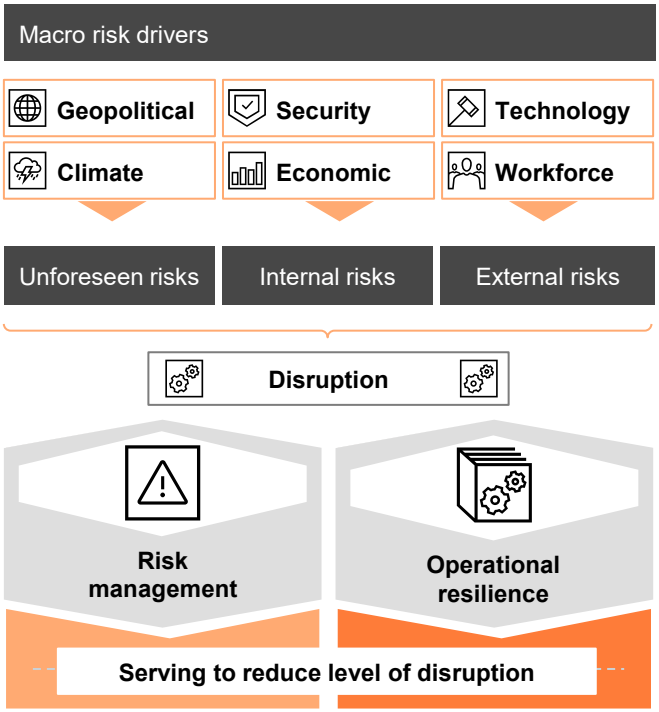
Just as importantly, how can both perspectives be embedded into decision-making processes, rather than viewing them in isolation?

Operational resilience

Has a **service or product-first lens** to assess the cumulative effect of impacts on critical services and products during disruption, by identifying and remediating vulnerabilities to remain within impact tolerance.

Risk management

Has an **objective-led lens** where associated risks are identified and assessed. Risk practitioners must implement suitable preventative and mitigating controls to manage risks within the defined risk appetite..



Integrate: Realise the benefits of unified risk and resilience

Operational resilience and risk management share the underlying objective of understanding potential vulnerabilities and strengthening the control environment to effectively manage risks and mitigate impacts to a firm's operations within acceptable levels.

Benefits of risk and resilience integration.

Streamlined identification and assessment activities

Feedback loops between risk and control assessments and operational resilience scenario testing improves identification of early warning signals, vulnerabilities and critical controls.

Monitoring and reporting synergies

Subject to existing system integration capability, combined risk and resilience dashboards improve data quality, with traceability through critical services and products, processes, risks and controls.

Improved confidence and assurance

Targeting resources towards activities that provide the best return on assurance (e.g. assurance over controls that support key risk and resilience outcomes).

Cultural reinforcement and cross skilling

Improves cross-pollination of risk and resilience resources to enhance capability and reduce duplication of effort across the first and second lines of defence.

The first step to realising these benefit is through building a resilient 'bowtie'.

The intersection of risk and resilience can be considered through the concept of the 'bowtie' model below. Most practitioners are familiar with the bowtie concept of risk and control – but understanding how resilience intersects with the model can help firms to tie the bow together.

Consider the risks and controls **mapped to deliver an organisation's critical services and products,** and how they are managed to: **a)** not only prevent disruptions **(left side of the bow tie)** that challenge an organisation's resilience posture; but **b)** also **mitigate impacts** of consequences from disruptive events **(right side of the bow tie).**

Current focus on risk management

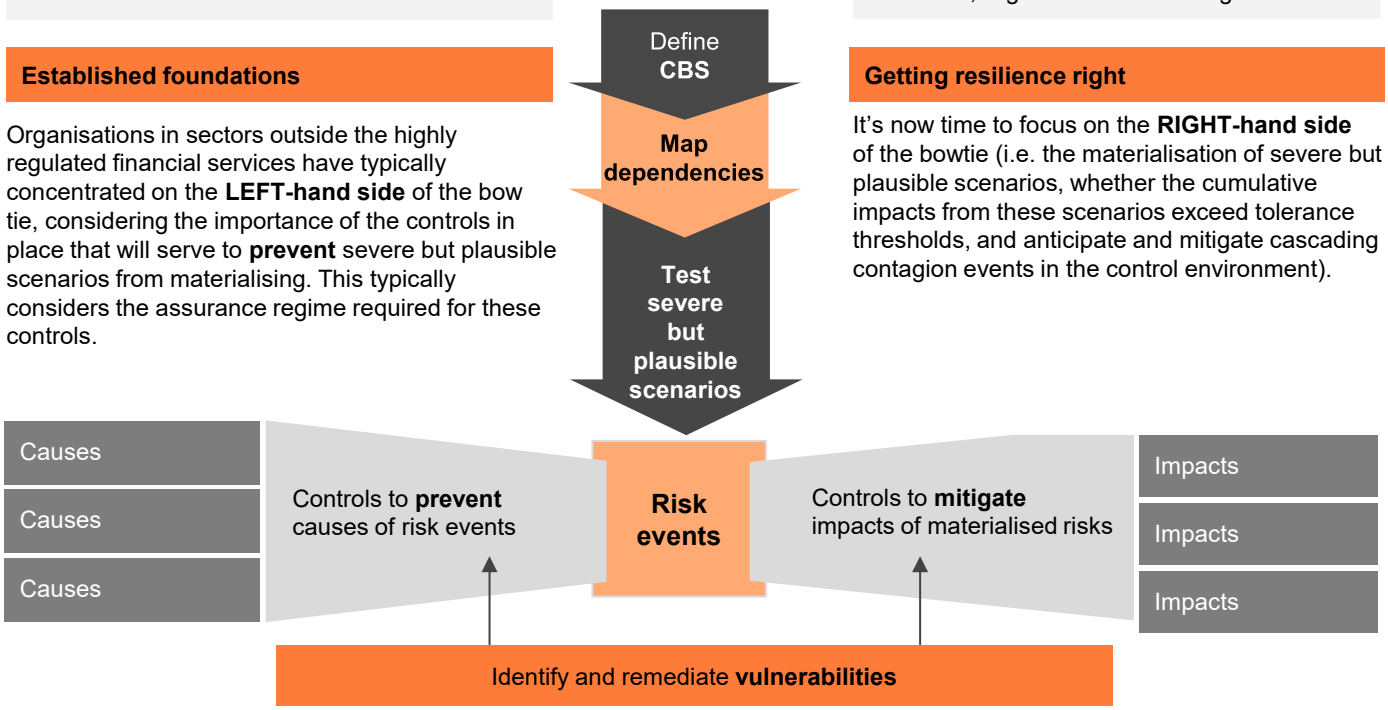
Future focus to enhance operational resilience, aligned with risk management.

Established foundations

Organisations in sectors outside the highly regulated financial services have typically concentrated on the **LEFT-hand side** of the bow tie, considering the importance of the controls in place that will serve to **prevent** severe but plausible scenarios from materialising. This typically considers the assurance regime required for these controls.

Getting resilience right

It's now time to focus on the **RIGHT-hand side** of the bowtie (i.e. the materialisation of severe but plausible scenarios, whether the cumulative impacts from these scenarios exceed tolerance thresholds, and anticipate and mitigate cascading contagion events in the control environment).



Elevate: Optimise risk and resilience integration

Connecting risk and resilience

Integrating risk and resilience means aligning frameworks, operating models, technology, and resources to enable a joined-up approach. Building a future-ready capability requires a long-term strategy that embeds resilience into broader strategic, risk, and control objectives and rethinks how the programme connects with wider risk functions. With senior leadership support, the second line may need to play a more hands-on role in helping the first line strengthen controls aligned to the delivery of critical services and/or products.

01 Strategy and framework

- Update risk management and resilience frameworks (whilst not conflating the two disciplines) to a) position risk and resilience as an integrated solution, and b) articulate how operational resilience is an outcome of effective risk management.
- Improve control frameworks to determine: a) how mapping critical services and/or products impacts the criteria applied to key control scoping. b) the assurance requirements over controls that mitigate risks within processes to deliver critical services and/or products.

02 Risk and resilience process and activities

- Develop an approach to determine how risk assessments impact the delivery of mapped critical services and/or products.
- Leverage risk assessments when scenario testing the recovery of critical services and/or products.
- Use resilience scenario testing outcomes to review linked risk profiles or controls in continuous monitoring methodologies.
- Map risks and controls to the delivery of critical services and/or products.
- Consider the integration of scenario testing and operational risk stress testing.

03 Roles and responsibilities

- Revisit mandates across the three lines of defence, taking into consideration collective risk and resilience objectives.
- Update lines of defence RACI with services provided across risk and resilience activities.
- Cross-pollinate risk and resilience resources, with skill requirements documented to support revised operating model mandates and service delivery structure.
- Articulate responsibilities of individual stakeholders for the management of risk and resilience, and streamline functions where risk and resilience can be combined.

04 Management information (MI) and reporting

- Streamline MI reporting processes to eliminate duplication and facilitate thorough and accurate data analysis, thereby minimising any contradictions in reports.
- Integrate risk and resilience reporting views to aid decision making for combined management of risk and critical services and/or products.
- Utilise horizon scanning capabilities to monitor the firms environment, and any emerging risks and vulnerabilities.

Underpinned by a integrated technology view

Technology platforms across risk and resilience disciplines help organisations anticipate, manage, and recover from threats. When integrated, these tools can unify risk and resilience functions around what matters most.

1. Take an integrated approach by connecting risk systems (e.g. GRC platforms) with resilience tools to create a unified view across critical services and/or products.
2. Review supporting system architecture to improve data quality and facilitate traceability through critical services and/or products, processes, risks, controls, and vulnerabilities.
3. Use technology to enable end-to-end visibility – from horizon scanning to recovery – supporting proactive prevention and informed response during disruptions.

Respond: Adopt a substitution approach during disruption

Organisations must also assess how substituting controls during disruption affects risk and resilience. A flexible, informed strategy is needed to adapt the BAU control environment while continuing to manage risk through disruption. The impact of substitutions on control effectiveness and resilience outcomes should be considered in advance – built into response plans and scenario testing, not left to be decided in a crisis.

Substitution approach – A case study

A substitution approach during disruption might involve switching to an alternative supplier if a primary one fails. For example, if a manufacturing firm's key transport provider experiences a system outage, it could activate a pre-identified secondary provider or in-house contingency to maintain service. This helps to establish continuity, reduce single points of failure, and strengthen resilience.. However, such substitutions may impact the BAU risk and control environment – so the cost-benefit of each option should be carefully assessed.

Third-party risk management – Increased reliance on multiple suppliers requires enhanced due diligence, ongoing monitoring, and contractual arrangements to facilitate alternative providers meeting the same risk and resilience standards as the primary supplier.

Operational complexity – Managing multiple suppliers introduces additional complexities in procurement, logistics, and integration, which may create new risks related to consistency, data security, and service quality.

Testing and assurance – The effectiveness of the substitution strategy must be regularly tested through scenario planning and operational resilience exercises to enable seamless transitions in real-time disruptions.

Cost and resource allocation – Maintaining secondary suppliers may introduce additional costs, requiring firms to balance resilience investments against efficiency considerations within their risk appetite.

Data and technology integration – The business must ensure that alternative suppliers can seamlessly integrate with existing systems without compromising data integrity, cybersecurity, or service continuity.

Control environment adjustments – Controls must be updated to reflect changes in workflows, enabling governance frameworks, risk assessments, and incident response plans account for substitution strategies.

Questions for risk and resilience practitioners to consider when flexing the BAU environment during disruption

Within risk environment

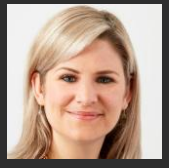
- How does a substitution approach impact existing risk exposures?
- Are we operating within our risk appetite?
- Are our controls adequate and effective?
- How do we monitor exposure and control? Is this covered by existing indicators (e.g. KRIs, KCIs)?

Within the resilience environment

- How does the adoption of a substitution method affect the efficiency and effectiveness of service delivery?
- How resilient are controls under stress?
- Have response plans been updated to include scenarios where substitution approaches are required?

Get in touch

Dave Stainback
Global Crisis and Resilience Co-Leader, PwC United States
+1 678.419.1355
david.stainback@pwc.com



Bobbie Ramsden-Knowles
Global Crisis and Resilience Co-Leader, PwC United Kingdom
+44 (0)7483 422701
roberta.ramsden-knowles@pwc.com

Contributors
Alex Sagovsky
alexander.sagovsky@pwc.com
Johanna Peterson
johanna.peterson@pwc.com
Callum Bright
callum.b.bright@pwc.com