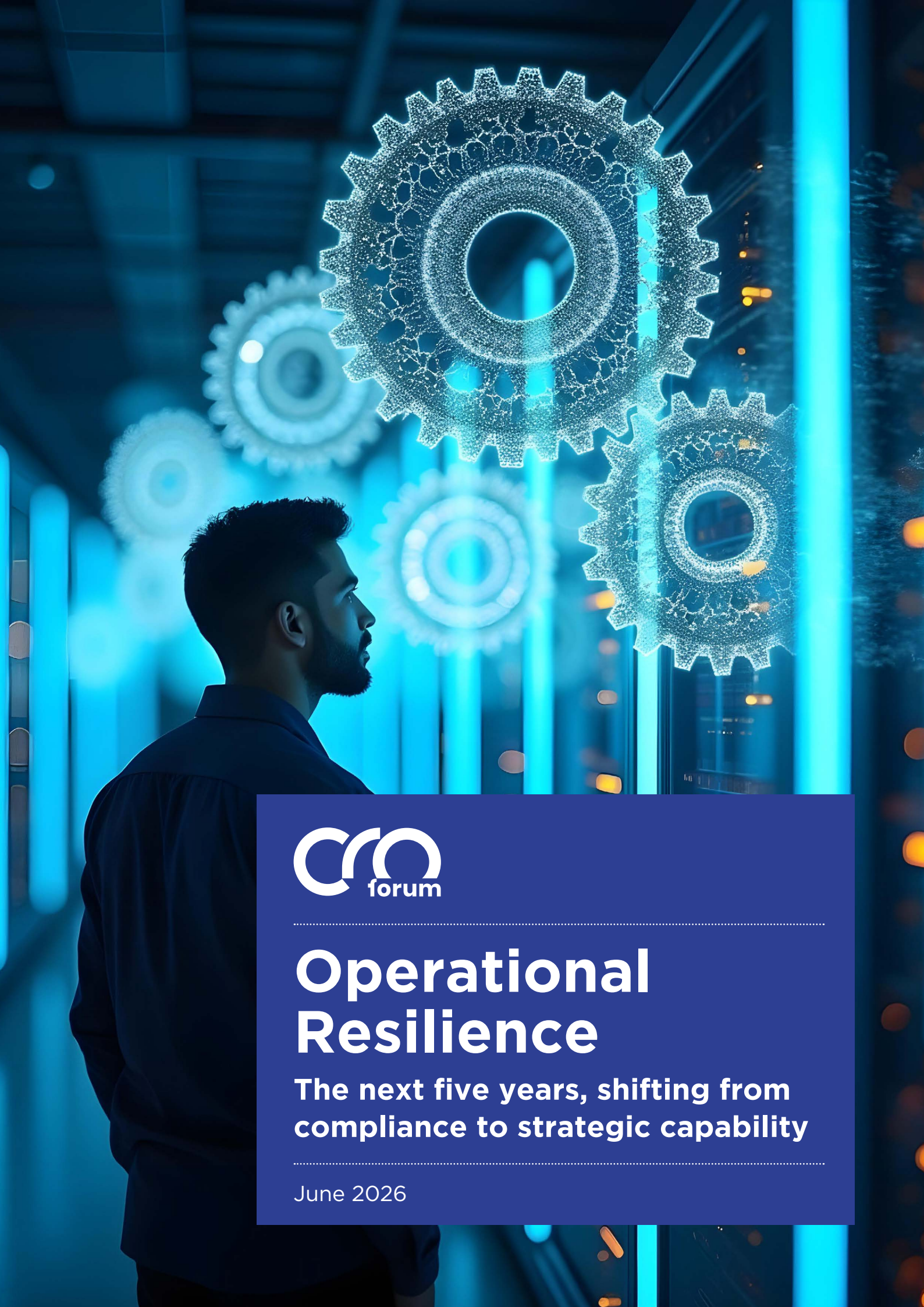


cro forum

Operational Resilience

The next five years, shifting from compliance to strategic capability

June 2026

Table of contents

cro forum

Executive summary

Purpose

The purpose of this paper is to provide a strategic, insurance-sector perspective on the evolving operational resilience landscape, highlighting the key risks, regulatory expectations, and practical considerations that will shape resilience maturity over the next five years.

Drawing on regulatory developments, industry surveys and insights from CRO Forum members, the paper aims to support Chief Risk Officers and senior leaders in strengthening operational resilience outcomes – protecting policyholders, sustaining critical insurance services and enhancing trust.

The CRO perspective

Thoughts from Shawn Gamble, M&G plc CRCO

"Operational resilience sits at the heart of effective risk management because it forces organisations to confront a simple but fundamental question: can we continue to deliver our most critical services no matter what? For (re) insurers, a sector that serves millions of customers and clients who rely on us for their financial security – this is not a theoretical challenge, it is an essential part of our duty of care. Operational resilience requires more than strong controls; it demands an enterprise wide understanding of our vulnerabilities, dependencies, and tolerances, and a culture in which risks are anticipated and managed before they become incidents. As CRCO, I see operational resilience as a unifying framework that connects our risk disciplines, ensuring we focus on outcomes, not just processes.

From a Risk function perspective, the importance of operational resilience lies in the transparency and discipline it brings. It elevates conversations beyond individual risk types – technology, cyber, third parties, change and people – and instead asks whether the end to end system can withstand disruption. This perspective matters because most operational failures occur at the intersections: where ownership blurs, dependencies are opaque, or governance has gaps. A mature operational resilience framework strengthens our ability to assess these cross cutting risks, challenge management on readiness, and provide boards and regulators with confidence that the firm can absorb shocks without harming customers or markets. Ultimately, resilience is not a compliance exercise; it is a strategic risk capability that protects trust in both our firm and the wider financial system."

Key themes & recommendations

Operational resilience is a core strategic outcome, with board-level accountability for its success. Firms must position operational resilience as an enabler of sustainable growth and transformation.

Global regulatory expectations are rising, as is the associated cost of compliance. Firms must implement a single unified framework that is applicable globally but applied locally.

Third parties and the broader supply chain represent systemic concentration risks to the sector. Firms must holistically assess the third- and nth- parties critical to its business operations and determine the associated concentration risk and subsequent firm-specific management actions.

Data is both a critical dependency that can immobilise critical services and fundamental to gaining assurance over a firm's operational resilience. Firms must embed data resilience by design – prioritising data integrity, recoverability and availability.

Testing requires a multifaceted approach, incorporating both firm-led and sector-led testing, across a range of severe but plausible scenarios – recognising the systemic threats posed by the sector. Firms should set out their testing strategy, ensuring testing is conducted end-to-end, and move away from siloed component-based testing.

The threat landscape is dynamic, and firms must continue to monitor, prepare and adapt to disruption to remain resilient. Firms must plan for systemic, sector-wide disruptions and understand how they will respond and recover.

Frameworks alone do not achieve operational resilience – governance (Board accountability), culture (tone from the top) and capability (cross-functional response and recovery) are fundamental. Firms must maintain the importance of these in their broader operational resilience frameworks.

1. Introduction

Operational resilience is the measurable ability to keep critical services running at acceptable levels through disruption. For insurers, it is essential to protecting policyholders, honouring long-term commitments and preserving trust — the very basis of the business.

Resilience in the insurance sector has evolved from basic disaster recovery and contingency plans into an enterprise-wide discipline. Successive shocks (for example, natural catastrophes, systemic market failures, major cyber incidents and the COVID-19 pandemic), exposed hidden interdependencies and made clear that resilience must be a Board-level priority, with real-world and costly impacts if firms fail to properly manage and (govern, test and resource) it. Regulators now expect firms to demonstrate preparedness across people, processes, technology and the wider ecosystem.

Operational resilience is best viewed as an outcome, not a function. It emerges from the coordinated management of multiple risk types: cyber and technology risks, third-party and supply-chain exposures, process and human error, legal and compliance constraints, physical threats and certain financial risks such as liquidity stress during claims surges. A firm's risk appetite gives the outcome direction, which, together with an understanding of the levels of harm that could be incurred by policyholders, helps define impact tolerances for critical services, and guide the prioritised investment between prevention, response and recovery capabilities. Translating appetite into concrete, measurable tolerances — and testing those limits — is the practical way to align resources with what matters most to policyholders and regulators.

Insurers occupy a unique dual role with respect to operational resilience. They are critical enablers of societal and economic recovery, providing financial protection, liquidity and certainty to households, businesses and markets when disruption occurs. At the same time, insurers must themselves remain operationally resilient, ensuring the continuity of critical services such as claims handling, policy administration, customer communications, payments and reinsurance settlements during periods of severe stress. Failure to do so can compound harm, delay recovery across the wider economy and undermine confidence in the insurance system. This dual responsibility heightens supervisory expectations and reinforces the need for insurers to design, test and govern operational resilience not only to withstand disruption, but to support recovery when resilience is needed most.

Delivering resilience rests on interlocking foundations. Business continuity management identifies critical services, maps dependencies and embeds realistic, routinely tested recovery plans. Cyber resilience layers prevention, detection, response and recovery to protect confidentiality, integrity and availability. Technology resilience focuses on architecture that supports redundancy, graceful degradation and measurable recovery objectives. Crisis management provides clear command structures, communication discipline and decision rights for rapid, coordinated action. Above all, third-party resilience extends these expectations beyond the enterprise: rigorous supplier governance, contractual standards, concentration controls and joint rehearsals are essential to reduce external single points of failure.

For executive risk officers the immediate task is clear, work with the Board and the Executive to ensure clear accountability and ownership for operational resilience as a strategic outcome – set the clear tone from the top and enable those on the ground to drive operational resilience as a priority throughout the organisation. They should challenge delivery teams to ensure continuity of critical services, push the organisation to prioritise material dependencies including third- and nth-parties, help align investment with the greatest vulnerabilities and ensure mature, end-to-end testing is conducted regularly and consistently, so the business can meet its obligations to policyholders in an increasingly interconnected world.

2. Global regulatory landscape

2.1 Introduction

Regulation has become one of the strongest forces shaping operational resilience across the (re) insurance sector. Supervisors worldwide are raising expectations, driving (re)insurance firms to enhance governance, testing, dependency mapping and third-party oversight. Globally, (re)insurers play a vital role in the financial stability of a country's economy, so much so that, in Germany, the insurance sector is considered part of the country's critical national infrastructure. For all (re)insurers, the cost and complexity of compliance continue to grow, whilst regulatory requirements place policyholder protection and the mitigation of systemic impacts firmly at the centre of (re)insurers' priorities.

While there is broad alignment in regulatory intent – focusing on critical services, impact tolerances, governance and resilience testing – jurisdictional divergence remains in terminology, scope and supervisory intensity (e.g., rules-based vs principles-based regulation). These differences require (re) insurers to make deliberate choices about how best to design a coherent operational resilience framework that can demonstrate compliance across multiple regulatory regimes. The challenge, and opportunity, lies in building a global model that is flexible enough to meet local expectations while maintaining consistency, efficiency and strong outcomes for policyholders.

Global regulations present both a compliance challenge and a strategic opportunity to enhance trust, safeguard policyholders and future-proof operations in an increasingly complex and regulated environment.

2.2 Operational resilience regulation overview

Globally, operational resilience regulations are generally aligned in intent and direction; however, differences in terminology, scope and application must be managed to ensure compliance with regulations. Key themes include:

- **Board accountability and governance:** senior management/boards are expected to own the resilience framework, oversee its implementation, testing and gap remediation.
- **Service-centric resilience:** planning should focus on critical services or operations where recovery tolerances are captured.
- **Critical dependencies:** there should be visibility into critical dependency across operational assets such as critical teams, locations, IT applications and third parties.
- **Scenario testing and continuous improvement:** regular, risk-based testing and exercising using severe but plausible scenarios.
- **Third-party reliance:** ongoing management of critical third parties, including controls for third-party risks and concentration exposures.

Some key jurisdictional call outs include:

- **European Union (EU):** Rules-based regulation, focused on ICT and driving a high degree of standardisation of requirements in various technical standards.
- **United Kingdom (UK):** Principles-based regulation, anchored on critical services and impact tolerances (time-bound metrics), evidenced through regular scenario testing.
- **Singapore:** Principles-based guidelines, based on a service-centric view, establishing associated service recovery time objectives and evidencing through testing.
- **Malaysia:** Rules-based policy document with detailed testing requirements, governance structures and notification rules.
- **Canada:** Principles-based guidelines, anchored on critical operations, with tolerances for disruption and explicit scenario testing expectations.
- **United States and Switzerland:** no dedicated operational resilience regulation for (re)insurers at present. In the case of the US, there is a higher appetite for deregulation.

Institutions face the risk of duplication across jurisdictions due to parallel assessments, multiple dependency mappings, differing testing requirements and variations in reporting requirements. This fragmentation increases workload, reduces consistency and weakens overall resilience effectiveness.

2.3 Recommendations

To meet multiple regulatory expectations efficiently, the recommendation for firms is to consider adopting a single, coherent framework built on:

- Unified governance and oversight with clear accountability at Board level and senior management.
- Common taxonomy of critical services and the setting of impact tolerances.
- Central resilience repository mapping critical dependencies, such as processes, teams, locations, IT applications and third- and fourth-parties.
- Creation of operational resilience plans including contingency strategies and roles during a disruption.
- Conducting severe but plausible scenario-based exercises and performing tests with relevant functions (for example, IT resilience and third-party management functions to check on consistencies and risk tolerances.
- Understanding how dependency failures affect delivery and embedding continuous improvement.

A harmonised framework minimises duplication, ensures regulatory consistency and strengthens the organisation's ability to anticipate, withstand and recover from disruptions across jurisdictions.

Insurers are increasingly integrating operational resilience insights into their enterprise frameworks, recognising that resilience is not just about recovery, it is about maintaining trust, protecting policyholders and ensuring continuity of critical services. As the regulatory landscape evolves, insurers must navigate a complex web of state mandates, national standards and global expectations to build truly resilient operations.

2.4 Jurisdictional breakdown

Introduction to selected key regulations (non-exhaustive) across jurisdictions that deal with operational and/or digital operational resilience, as well as associated topics such as operational risk management, business continuity management and IT resilience.

EUROPEAN UNION
Digital Operational Resilience Act (DORA)

The European Union's (EU's) Digital Operational Resilience Act (DORA) aims to ensure EU financial entities remain digitally resilient, maintaining service quality and reliability even during disruptions. The regulation applies to regulated financial institutions, other financial information providers and Information and Communication Technology (ICT) service providers supporting financial services. (Re) insurers were required to adhere to the regulation since 17 January 2025.

DORA is built on five core pillars of ICT risk mitigation:

1. **ICT risk management:** strong governance, continuous risk identification and protection measures
2. **Incident management and reporting:** robust response and mandatory authority reporting
3. **Resilience testing:** regular testing, including Threat-Led Penetration Tests (TLPT)
4. **Third-party risk:** oversight of suppliers, contracts and exit strategies
5. **Information sharing:** voluntary exchange of cyber threat intelligence

Recent supervisory focus areas and enhancements under DORA include:

- Simplifying rules and standardise requirements across all EU financial entities
- Applying controls based on size, risk and complexity
- Focusing on entity-level requirements, extendable to groups
- Strengthening roles of EU and national supervisors
- Imposing detailed compliance efforts, especially for less mature entities
- Promoting stronger resilience and information sharing
- Placing critical third-party providers under EU supervision

With DORA, the EU has established a unified regulatory foundation for operational resilience, ensuring a consistent and standardised approach across member states through a series of binding technical standards. The Critical Third-Party (CTP) designation for DORA has now gone live, with 17 relevant CTPs identified.

UNITED KINGDOM

Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA) and Bank of England

UK Regulators PRA (SS1/21) and FCA (PS21/3) consider that for firms to be operationally resilient, they should be able to prevent disruption to the extent practicable, adapt systems and processes to continue to provide services and functions in the event of an incident, return to normal running promptly when a disruption is over and learn and evolve from both incidents and near misses. Operational resilience is an outcome that is supported by several parts of the UK regulatory framework, in particular

- Governance
- Operational risk management
- Business continuity planning
- Management of outsourced and third-party relationships

UK-regulated firms must identify their important business services, set and document impact tolerances for each and ensure they can remain within these tolerances during severe but plausible disruptions – with tolerances focused on intolerable harm to customers, clients and policyholder protection, as well as risks to firm safety and soundness and, in some cases, risk to the stability of the UK financial system.

In March 2026, the FCA, PRA and Bank of England published new rules on operational incident reporting and material third-party arrangement reporting. These updates relate to mandating a standardization in incident reporting and thresholds for reporting focused on customer, client and market harm and risks to firm safety and soundness, as well as expanding previous outsourcing-focused regulation to cover all material third parties.

SWITZERLAND

Eidgenössische Finanzmarktaufsicht FINMA

FINMA issued its circular 2023/1 Operational risks and resilience – banks on 7 December 2022, which replaced the previous circular 2008/21 Operational risks – banks. The circular entered into force 1 January 2024 and is focussed on banks, securities dealers and banking groups and does not yet include (re)insurers. However, FINMA also intends to revise (re)insurance supervisory ordinance and associated circulars and is likely to align with circular 2023/1 issued for banks.

Whilst requirements for (re)insurance companies are still focused on business continuity management; FINMA is currently working on an update of these regulations.

SINGAPORE
Monetary Authority of Singapore (MAS)

The MAS issued its revised Business Continuity Management Guidelines on 6 June 2022 and full compliance was expected by 6 June 2023. The purpose of the Guidelines is to ensure that Financial Institutions (FIs) remain resilient to service disruptions and can continue delivering critical services to customers. They apply across the financial sector in Singapore, including banks, insurers, fund managers, brokers and other MAS-regulated entities. Key principles towards FIs include:

- Adopt a service-centric approach, focusing on the timely recovery of critical services facing customers.
- Identify end-to-end dependencies, for example people, technology and third parties, that support critical services and address any gaps that could hinder recovery.
- Enhance threat monitoring, environmental scanning, regular testing and audits and maintain governance and management oversight.

In terms of business continuity and operational resilience, the Guidelines require FIs to:

- Identify critical business services and set recovery objectives, for example Service Recovery Time Objective (SRTO).
- Map dependencies supporting those services, including internal and external services.
- Establish a business continuity plan with clear roles and responsibilities, activation triggers and escalation procedures.
- Adopt a testing programme that is commensurate with the criticality of services, including exercises, internal audits at least every three years.
- Monitor compliance and provide senior management attestation or Board reporting as required.

MALAYSIA
Bank Negara Malaysia (BNM)

BNM issued its Business Continuity Management (BCM) Policy Document on 19 December 2022 and the majority of requirements came into effect 19 December 2023, with certain Disaster Recovery (DR) testing clauses from 19 December 2025, for Malaysian-licensed financial institutions. The policy is designed to strengthen operational resilience in Malaysian financial institutions by ensuring continuity of critical business functions and critical services under disruption.

Major components of the policy towards FIs include:

- Establish a governance framework with clear accountability (Board, senior management, BCM committee) for business continuity.
- Conduct risk assessments and Business Impact Analyses to identify Critical Business Functions and determine objectives such as Maximum Tolerable Downtime and Recovery Time Objectives.
- Develop and maintain a set of plans: a Crisis Management Plan, a Business Continuity Plan and a Disaster Recovery Plan, covering internal operations and outsourcing arrangements.
- Address dependencies, including people, technology, data, locations and third- and fourth-parties in plans and include testing, communication and stakeholder engagement features (including regulator notification for cyber and non-cyber incidents).

AUSTRALIA

Australian Prudential Regulation Authority (APRA)

APRA issued the Prudential Standard CPS230 Operational Risk Management in June 2024, which replaced Prudential Standards CPS 231 Outsourcing and CPS232 Business Continuity Management. The standard came into force on 1 July 2025. CPS230 aims to ensure that every APRA-regulated entity is resilient to operational risks and disruptions. It applies across the financial sector: authorised deposit-taking institutions, insurers (life, general and private health), superannuation trustees and Registrable Superannuation Entities licensees.

Major guiding principles under the standard are:

- Entities must effectively manage operational risks, set and maintain appropriate standards for conduct and compliance.
- Entities must maintain their critical operations within defined tolerance levels during severe disruptions.
- Entities must manage the risks arising from the use of service providers, including third parties.

The standard requires entities to list their critical functions and review them annually. The framework should consist of the following components:

- Define and maintain a register of critical operations and set tolerance levels.
- Collect and maintain capabilities, such as critical people, resources, technology.
- Create a business continuity plan with roles and responsibilities, triggers for activation and action to maintain operations.
- Follow a testing programme with annual business continuity exercises, covering severe but plausible scenarios.
- Follow up on findings, with associated actions formally tracked.
- Report test results and findings such as remediation needs, to the Board.

CANADA

Office of the Superintendent of Financial Institutions (OSFI)

Canada's Office of the Superintendent of Financial Institutions issued the final Guideline E-21 Operational Risk Management and Resilience on 22 August 2024. Financial institutions were expected to immediately comply with to operational risk management expectations in sections 1 and 2. A phased implementation approach applies to other expectations in the guideline, with full adherence and operationalisation by 1 September 2026.

Operational resilience entails a sound understanding of critical operations end to end and their delivery through severe but plausible circumstances within established tolerances for disruption. The guideline requires entities to list their critical operations, which should be reviewed regularly. The following components are suggested:

- Identify and maintain a list of critical operations and establish tolerances for disruption.
- Collect and maintain a list of critical people, technologies, processes, facilities, third parties and dependencies.
- Perform scenario testing based on identified vulnerabilities.
- Have processes in place to address gaps identified during testing.

Robust operational risk management and resilience enhance the ability to prevent, detect, respond to and recover from adverse events, while continuing to deliver critical operations.

UNITED STATES

State-level authorities, National Association of Insurance Commissioners (NAIC)

Unlike banks, insurers are regulated by individual US state Departments of Insurance, each of which sets its own expectations for business continuity, cybersecurity and risk management. The National Association of Insurance Commissioners (NAIC) plays a central role in harmonising these efforts through model laws and guidance. Notably, the NAIC's Insurance Data Security Model Law (MDL-668) has been widely adopted across states, requiring insurers to implement comprehensive cybersecurity programs, conduct risk assessments and report data breaches. While not explicitly labelled as operational resilience, these requirements form the backbone of resilience planning.

At the national level, insurers increasingly align with best practices from federal agencies and global standard-setters. The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Guidelines and more recent updates signal a shift toward frameworks like NIST Cybersecurity Framework 2.0 and CISA Cybersecurity Performance Goals, which many (re)insurers are now adopting. These tools help insurers assess their resilience posture across critical domains such as third-party risk, incident response and governance.

Globally, the International Association of Insurance Supervisors (IAIS) has elevated operational resilience as a strategic priority. Its 2023 issued paper on insurance sector operational resilience outlines key vulnerabilities, including IT failures, outsourcing risks and cyber threats.

3. Third-party resilience and concentration risk

3.1 Introduction

In today's increasingly interconnected world, (re)insurers are more reliant than ever on third-party providers for critical services such as IT infrastructure, data processing and cloud computing, with specialist outsourcing providers providing a range of administrative and expert services that can be leveraged by firms. These third parties are often deeply embedded in the processes that underpin a firm's ability to serve its customers, meet regulatory obligations and maintain its operational continuity. These associated dependencies introduce a range of risks that can significantly impact the operational resilience of firms.

In a recent survey carried out by the CRO Forum, 100% of respondents named third-party resilience (including nth-parties) as either important (32%) or very important (68%) to their operational resilience framework, while 86% of respondents named third-party resilience and concentration risk as a key area of focus for their operational resilience between 2026 and 2030.

A pressing concern for many is the concentration risk stemming from the widespread adoption of hyper-scale cloud providers. While these platforms offer scalability and efficiency, they also create potential single points of failure. A disruption at a major cloud provider could simultaneously affect multiple (re)insurers – both through direct service contracts and indirect dependencies as sub-providers of others, posing systemic risks across the financial sector.

The degree to which (re)insurers rely on third parties varies significantly depending on their strategic orientation. Some firms pursue a leaner, more outsourced operating model to increase agility and reduce costs, while others retain more functions in-house to maintain control. These strategic choices directly influence the institution's risk profile and the complexity of its operational resilience and third-party management frameworks.

Traditionally, Third-Party Risk Management ("TPRM") has sought to effectively manage associated risks and ensure alignment with firms' risk appetite. Third-party resilience moves beyond third-party risk management by working to ensure that third parties are resilient and able to withstand incidents and disruption, ensuring that services can continue to be provided within firms' risk appetites.

To deal with the challenges of today's complex landscape and ensure third-party identification (mapping), the effective management of traditional related risk and assess associated resilience, there is an opportunity for firms to look at building out their existing frameworks beyond foundational elements such as risk assessments, due diligence and contractual protections to include additional resilience related controls, such as real-time monitoring, resilience testing, incident response planning and exit strategies.

Global best practices emphasise that resilience is proactive: organisations cannot outsource accountability for continuity. Failures at critical third parties, such as CrowdStrike, have led to severe financial and reputational damage in recent years, underscoring why resilience must be embedded into contracts, but must also continuously assessed and managed by the (re)insurer itself. Regulatory initiatives worldwide underscore and reinforce this expectation, turning third-party resilience into a cornerstone of operational stability and competitive advantage.

3.2 Mapping dependencies & risk aggregation

Mapping third-party dependencies is essential for operational resilience. It provides visibility into external services and processes that underpin critical operations, helping firms identify single points of failure, understand complex interdependencies and comply with regulatory requirements such as the EU's Digital Operational Resilience Act ("DORA"). Without this clarity, (re) insurers cannot accurately assess vulnerabilities or prepare for disruptions.

To do this effectively, (re)insurers should, taking a risk-based approach:

- Map all dependencies, including indirect relationships via sub-contractors.
- Identify critical third-party relationships.
- Prioritise third-party management activity based on criticality, defined by potential business impact.
- Integrate mapping into risk frameworks, aligning with Business Impact Analyses and resilience testing.

A robust mapping process is systematic, collaborative and regularly updated.

Scenario testing and incident reviews should be used to update and refine dependency data. Outputs of dependency mapping should be integrated into the third-party framework to ensure that risk assessments, contract reviews and assurance activity mirror the firm's dependency on the third-party. Additionally, these insights strengthen the identification and management of potential vulnerabilities.

3.3 Incorporating third-party resilience into third-party risk management

To effectively manage third-party risk and drive third-party resilience, organisations should implement a suite of controls, within both their third-party and operational resilience frameworks to ensure that third-party dependencies identified in their mapping are appropriately managed, including:

Risk-based onboarding and due diligence: Assess third parties based on their criticality and potential impact, involving relevant functions and experts. Ensure that due diligence considers resilience appropriately (e.g., information security assessments could consider ability to recover from a cyber incident as well as a third-party's ability to safeguard data processed on behalf of the firm).

Contractual safeguards: Embed resilience-related clauses (e.g., business continuity, incident notification, sub-contracting, testing and audit rights) into contracts, informed by due diligence results.

Ongoing monitoring and assurance: Maintain transparency regarding third-party dependencies, including for senior management and regularly review performance, conduct audits and test contingency plans. Consider implementation of real-time monitoring to support visibility of third-party resilience.

Scenario testing and exit planning: Prepare for plausible disruptions by testing the firm's business continuity, incl. critical third-party dependencies and exit strategies, considering workarounds and alternative providers.

Nth-party management: Understand and manage risks arising from your third parties' own suppliers, including Concentration Risk.

Continuous improvement: Use incidents and near misses, whether internal or external, as well as learnings from testing, to refine controls and enhance resilience.

The TPRM framework should define roles, responsibilities and structured processes for identifying, assessing and mitigating risks throughout the lifecycle of third-party relationships. Frameworks should be risk-based, enabling (re) insurers to categorise third parties based on the criticality of the services they provide. This allows for differentiated oversight and for firms to focus on those third parties they are dependent upon for the delivery of critical operations. Data collected by the CROF suggests that nearly all member firms take a risk-based approach to TPRM, with third-party frameworks linking criticality to the level of controls applied.

3.4 Concentration risk: What is it and how does mapping help?

Concentration risk in relation to third parties arises when a firm is overly reliant on a single supplier, technology, or geographic region. Regulations such as DORA support firms in developing a definition of concentration risk that is relevant to their operations and their supply chain. Concentration risk is an area of increasing concern and has been flagged in a recent survey by CRO Forum members as the second most prevalent threat to their supply chain, after cyber security risk. Mapping dependencies and identifying critical third-party dependencies enable firms to:

- Identify and quantify concentration risks.
- Develop diversification strategies (e.g., dual sourcing and alternative providers) or pursue active risk acceptance.
- Inform Board-level risk appetite and regulatory disclosures.

Effectively managing concentration risk is essential to safeguarding operational resilience and meeting regulatory expectations. Specific questions firms can consider to effectively assess and manage their concentration risk within their critical third parties to ensure alignment with risk appetite could include the following:

- Where do we have significant dependencies on a single third-party, fourth party, or geographic region and how are these identified and monitored?
- Do we have a dependency on any of the critical third-parties identified by the Regulators?
- Are we monitoring for “hidden” concentration risk, such as multiple third-parties relying on the same fourth or Nth party (e.g., cloud infrastructure providers)?
- How do we ensure our concentration risk does not exceed our stated risk appetite or regulatory expectations?
- What diversification (e.g., dual sourcing, alternative providers) and management strategies (e.g., exit planning) are available to mitigate concentration risk? Do we need to accept certain risks?
- How do we incorporate concentration risk into our scenario analysis, stress testing and operational resilience planning?

3.5 Sector-wide challenges

Full transparency across the supply chain is challenging due to complexity, commercial sensitivities and data limitations. Data collected by the CRO Forum shows that members are at differing points in their journey through their supply chains, aligned to organisational risk appetite. 45% of survey respondents are considering fourth parties, 25% fifth parties and beyond while 30% of respondents remain focussed solely on their third-party relationships and dependencies. Industry initiatives and shared data platforms are emerging to standardise and streamline third-party assurance. Regulators have also acted to support firms to manage systemic concentration risk through critical third-party regimes in both the EU and UK.

The European ESAs have released their list of Critical ICT Third Parties which will be managed by the Regulator under DORA; however, firms are expected to continue to manage relationships with these critical third parties according to their own existing frameworks. It is worth noting that regulators may suggest alternative providers for firms if concentration risk is felt to be systemic so having credible alternative providers identified is key for firms.

Outside DORA and ICT, the European ESAs do not have a list concerning critical third-party concentrations however, firms may also face concentration risk in such other areas (for example, claims TPAs, Loss adjusters or other experts) and should apply a consistent framework to addressing concentration risk across their entire supply chain.

3.6 Conclusion

Third-party failures can disrupt core (re)insurance operations, trigger regulatory breaches and damage customer trust. Concentration risk amplifies systemic vulnerabilities. A single outage can cascade across the financial sector, making resilience a Board-level concern rather than an operational detail.

Embedding resilience obligations directly into contracts is key. Service Level Agreements (SLAs) should clearly define recovery time objectives (RTOs), audit rights, incident reporting requirements, transparency around subcontracting arrangements and termination obligations with fixed notice period and exit support. For critical third parties, resilience testing must be a contractual requirement to ensure recovery capabilities are validated in practice rather than assumed. Conducting joint exercises with third parties helps validate contingency plans, uncover weaknesses before they become operational failures, provide a realistic measure of preparedness and strengthen collaboration with key providers.

Understanding and managing concentration risk is another priority but one without a one-size-fits-all approach. Aligned to their risk profile and appetites, organisations could consider working with providers to deliver active-active cloud options, across multiple regions, explore multi-cloud strategies, maintain backup providers and establish alternative processing pathways to avoid over-reliance on a single third-party or technology platform. Diversification across the supply chain helps mitigate concentration risk but also enhances operational flexibility and business continuity.

Finally, staying ahead of regulatory developments is essential. Firms must anticipate evolving requirements under frameworks such as DORA by embedding compliance throughout the third-party risk management lifecycle. Engaging with industry forums and regulatory working groups helps organisations align with emerging standards and maintain a proactive posture rather than reacting to new mandates.

Third-party resilience and concentration risk are no longer peripheral concerns — they are central to operational stability and regulatory compliance. CROs should consider championing a holistic approach that combines mapping and monitoring, contractual safeguards, proactive testing, diversification and regulatory intelligence, aligned to the risk profile of their firm. By doing so, firms can transform third-party risk management from a compliance obligation into a strategic enabler of resilience and long-term competitiveness.

4. Resilience testing

4.1 Introduction

Resilience testing is a core mechanism through which (re)insurers evidence that their operational resilience framework is effective in practice. It provides assurance that critical services and the dependencies that support them can continue to operate within defined tolerances during disruption. Regulatory regimes including the PRA and FCA operational resilience framework and the EU's Digital Operational Resilience Act (DORA) place increasing emphasis on structured, risk-based and repeatable testing.

Testing is not only a means to demonstrate compliance; it helps confirm that capabilities work under realistic conditions: controls operate as intended, recovery procedures are executable and decision-making under stress is effective. Just as importantly, testing supports continuous improvement by identifying vulnerabilities, informing remediation and refining scenario design.

Given the increasing complexity of threats, firms typically adopt a balanced testing strategy covering operational resilience, cyber resilience and (where relevant) financial resilience – supported by horizon scanning and intelligence-led insights. The sections below outline common approaches, from firm-led testing through to sector-led exercises.

4.2 Firm-led testing

Many firms structure a firm-led testing programme using complementary approaches, aiming to cover both component-level resilience (micro-resilience) and end-to-end service resilience (macro-resilience).

End-to-end and component testing

End-to-end (E2E) testing is often used to explore whether each critical service together with its supporting people, processes, technology, data and third parties can continue to operate within defined tolerances. In practice, tests commonly seek to evidence that:

- localised failures do not cascade into service-wide disruption
- failover mechanisms operate as expected
- recovery actions can be executed within tolerance

Component-level testing is typically applied on a risk-based basis and aligned to the criticality of the service. It helps firms build confidence that key dependencies (for example, applications, infrastructure components, data controls and operational procedures) can be relied upon under stress.

Scenario-based testing

Scenario-based testing typically simulates severe but plausible disruptions, drawing on real-world events, horizon scanning and sector intelligence. Examples include:

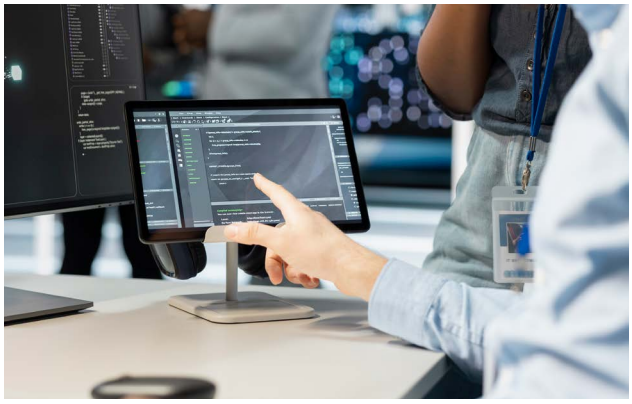
- large-scale cyber events (data corruption, ransomware and destructive malware)
- sudden loss of a critical third-party service
- regional outages (power, telecoms and cloud region failures)
- supply chain disruption
- hybrid cyber–physical incidents

Many firms involve senior management in these exercises to help validate command structures, stress decision-making and assess communication and escalation pathways. Outputs are often used to inform remediation activity and refine risk prioritisation.

Intelligence-led testing (including cyber TLPT)

Testing programmes are increasingly incorporating intelligence-led approaches. Threat-led penetration testing (TLPT) – including CBEST in the UK and DORA TLPT in the EU can help validate whether firms can detect, contain and recover from sophisticated threat actors.

These exercises can be integrated into the wider resilience testing strategy so that cyber resilience is considered alongside operational resilience tolerances and findings feed into remediation, governance and scenario design.



Testing third-party and nth-party dependencies

Given the material role of third parties in insurance operations, testing is often used to validate:

- the resilience of critical suppliers
- failover options such as backup providers, alternative processes, or dual sourcing
- the firm's own ability to operate during a third-party outage
- the realism of exit strategies under both stressed and non stressed conditions

Where appropriate, firms may conduct joint testing with critical suppliers to validate contractual obligations, data integrity, recovery procedures and communication pathways – recognising that feasible approaches can differ by firm and operating model.

Financial resilience testing

Complementary to operational testing, financial resilience testing can explore the firm's ability to absorb stress from:

- large claims surges
- market movements
- liquidity pressures
- the financial impact of prolonged operational disruption

Financial and operational scenarios are increasingly being considered together, reflecting the interdependence between prudential resilience and operational resilience.

Practical considerations for testing

- **Start with outcomes:** map test plans to defined impact tolerances for each critical service (for example, impact tolerances, maximum tolerable outage, maximum backlog, data integrity limits).
- **Prioritise by risk:** focus effort on services with high customer harm potential, high volumes, tight tolerances, complex dependency chains or known single points of failure.
- **Choose the least disruptive test that still answers the question:** use tabletop exercises to validate decision-making and playbooks; simulations and component tests to validate controls; and live end-to-end failover only where needed to evidence that tolerances can be met.
- **Scale frequency and depth:** increase cadence where services are most critical, change is frequent (for example major releases or outsourcing changes), or prior tests/incidents identified weaknesses.
- **Evidence remediation:** where issues are found, retest in a targeted and time-bound way to confirm fixes and demonstrate learning.
- **Prioritise by risk:** firms often focus effort on services with high customer harm potential, high volumes, tight tolerances, complex dependency chains, or known single points of failure.

Common challenges with testing

- **Cost:** delivering mature testing at scale can result in firms incurring significant costs (both the cost of the resources, but also the potential cost to incorporate additional stakeholders, such as third parties and any tooling required to perform the testing).
- **People and specialist capacity:** designing and executing meaningful tests typically requires scarce skills (service owners, operations SMEs, technology engineering, cyber, third-party management, risk/compliance, data). Peak demand often coincides with other regulatory delivery, major change and incident response.
- **Workforce disruption:** realistic exercises pull senior leaders and operational teams away from BAU. This is amplified for cross-functional tests that span multiple lines of business, time zones and suppliers.
- **Business disruption and customer impacts:** production-like testing can create outages, degraded service, increased error rates and backlog build-up. Even where customers are shielded, operational staff may be diverted into manual workarounds.
- **Technology environment constraints:** many firms lack representative, safely isolated test environments; data masking and privacy constraints can prevent "true" end-to-end rehearsal; and legacy estates may not support safe failover testing without material engineering effort.
- **Third-party coordination:** joint testing (and evidence collection) is limited by suppliers' willingness, commercial constraints, shared-tenancy architectures (e.g., cloud) and misaligned testing calendars. Nth-party visibility can be incomplete.
- **Evidence, documentation and auditability:** regulators expect traceability from services → dependencies → scenarios → results → remediation. Building and maintaining this evidence base is a recurring cost, not a one-off exercise.

Commonly feasible to test (with appropriate controls)

- **Component resilience:** backups and restores, failover/failback of applications and infrastructure, capacity and performance under stress and monitoring/alerting effectiveness.
- **Operational workarounds:** manual processes, prioritisation rules (e.g., claims triage) and backlog management under constrained capacity.
- **Data integrity and recoverability:** restoration of critical datasets, reconciliation controls and recovery point objectives in practice.
- **Third-party response integration:** incident communications with key suppliers, invocation of contractual obligations and validation of the firm's ability to operate through a supplier outage (including invoking alternative processes).

Often challenging (or not appropriate) to test "for real"

- Full-chain (nth-party) failure simulation: firms often cannot force or observe deep supplier ecosystems, particularly in shared-tenancy cloud environments or where commercial sensitivities restrict transparency.
- Some cyber scenarios in production: live ransomware or destructive malware simulation can create unacceptable risk to data integrity and firm safety and soundness; many controls must be validated in isolated environments.
- Cross-firm systemic events on demand: sector-wide cascades (telecoms collapse, cloud regional failure, FMI disruption) are difficult to rehearse as "live" events without regulator and industry coordination.

Test planning and the future landscape

To ensure that testing outputs are sufficient to evidence reasonable testing, firms should consider the following:

- Defined test objectives and success criteria (including what would constitute a tolerance breach and how it would be handled).
- Documented results (observations, timings, decision logs, evidence of control performance) and clear statements of scope/limitations.
- A prioritised remediation plan with owners and timelines and re-test plans where fixes is material.
- Governance reporting showing senior management and Board oversight, challenge and investment decisions informed by testing outcomes.

A more mature testing strategy often:

- is risk-based, using threat intelligence, horizon scanning and emerging risk insights to shape test themes
- considers shifts in technology, concentration risk, geopolitical context, climate risk and systemic dependencies
- incorporates both annual recurring tests and multi-year thematic exercises
- maps each test to the relevant impact tolerance or critical outcome

4.3 Sector-led testing

Sector-led testing can help firms understand resilience at a system-wide level and explore interconnections across the financial ecosystem. These exercises may provide insights into risks that can be difficult to identify through firm-only testing, such as:

- cross-firm dependencies
- systemic concentrations in cloud providers, telecommunications and r shared service platforms
- resilience of Financial Market Infrastructures (FMIs)
- cascading impacts from critical third-party failures
- the effectiveness of sector-wide coordinated responses
- improving customer and policyholder outcomes
- strengthening industry–regulator collaboration
- enhancing the realism of extreme but plausible scenarios
- complexity of coordinating firms with different operating models
- data sharing sensitivities
- resource demands across the sector

Participation in sector-led exercises can vary by jurisdiction, firm type and supervisory approach. In some cases, particular firms (e.g., certain Tier 1 institutions) may be expected to take part. The CRO Forum may also be able to support the development of future insurance sector-wide tests and industry playbooks.

Areas of consideration across the insurance industry

Insurers rely heavily on FMIs for claims payments, premium flows, market transactions and settlement activity. Testing can incorporate FMI recovery assumptions and plausible failure modes to explore:

- payment delays
- liquidity impacts
- cross-border settlement issues

The increasing reliance on a small number of technology and data providers continues to raise concentration risk. Testing can consider both firm-specific and sector-wide exposure and may incorporate:

- joint testing where feasible
- realistic workarounds
- alternative pathways for delivering customer outcomes

4.4 Role of supervisors

Regulatory bodies such as the PRA, FCA and ECB increasingly set expectations for firms to embed scenario testing within their operational resilience frameworks. Scenarios are commonly expected to be severe yet plausible, covering a range of threats including cyber-attacks, technology outages, third-party failures and environmental impacts. Governance is often a focus area, with boards expected to oversee scenario design and review remediation plans. In some parts of financial services, supervisors may also expect participation in sector-wide exercises, reflecting a growing emphasis on systemic resilience.

Initiatives such as the Bank of England's CBEST and sector-wide cyber resilience exercises demonstrate the value of collaborative testing. They highlight the importance of realistic scenarios that capture cross-border and third-party dependencies and the usefulness of clear playbooks to guide response and recovery. Post-exercise reviews can drive improvements in governance, communication and technical resilience, reinforcing that scenario testing is iterative and benefits from continuous refinement.

Exercises such as SIMEX, which explored a large-scale power outage, illustrate the potential value of coordinated response. They can reinforce the usefulness of shared playbooks for communication and escalation and the need to understand cross-sector dependencies, particularly with Financial Market Infrastructures (FMIs) and critical national infrastructure (CNI). Similar approaches could be considered for scenarios involving CNI or FMI failures, supported by joint planning between regulators, firms and infrastructure providers.

Testing expectations should be proportionate: not all firms will be in scope for every regulatory regime or exercise and firm-led programmes should reflect size, complexity and materiality.

Future testing models

Future models of resilience testing should move toward a coordinated insurance sector framework, drawing on banking sector maturity.

This includes:

- industry playbooks for macro-level disruptions
- cross-firm testing programmes for systemic threats
- greater use of threat intelligence to shape scenarios
- integration of financial and operational resilience testing
- multi-hazard, multi-vector scenarios combining cyber, climate, third-party and geopolitical drivers

These enhancements would strengthen confidence in the sector's ability to withstand extremes beyond historical experience.

4.5 Conclusion

Effective resilience testing demonstrates that a firm can remain within impact tolerances under disruption. A modern testing programme must increasingly be:

- risk-based
- intelligence led
- collaborative with third parties
- aligned to sector-wide risks
- integrated with financial resilience
- forward-looking, incorporating emerging threats

By refining testing strategies, enhancing joint and sector-led exercises and embedding lessons into governance and investment decisions, firms can develop a mature, adaptive and evidence based operational resilience posture.

5. The role of data

5.1 Introduction

It is not hyperbole to state that data is one of the most critical components of operational resilience. It not only itself is a foundational pillar of operational resilience (in that disruption to critical data dependencies can immobilise associated critical services, lead to intolerable harm and threaten firm safety and soundness), but it is also fundamental to being able to objectively assess the operational resilience of a firm (i.e., by validating the completeness and accuracy of key components of a framework – critical services identification, tolerance setting and breach monitoring and alerting, incident reporting, dependency mappings, testing outcomes, remediation effectiveness, etc.). Firms which strive for maturity in their use of data to strengthen operational resilience ought to consider two key components:

- The resilience of critical data dependencies (that is, data dependencies, without which critical services would not be able to operate or would be materially degraded).
- The application of data to assess and monitor operational resilience.

5.2 Data resilience

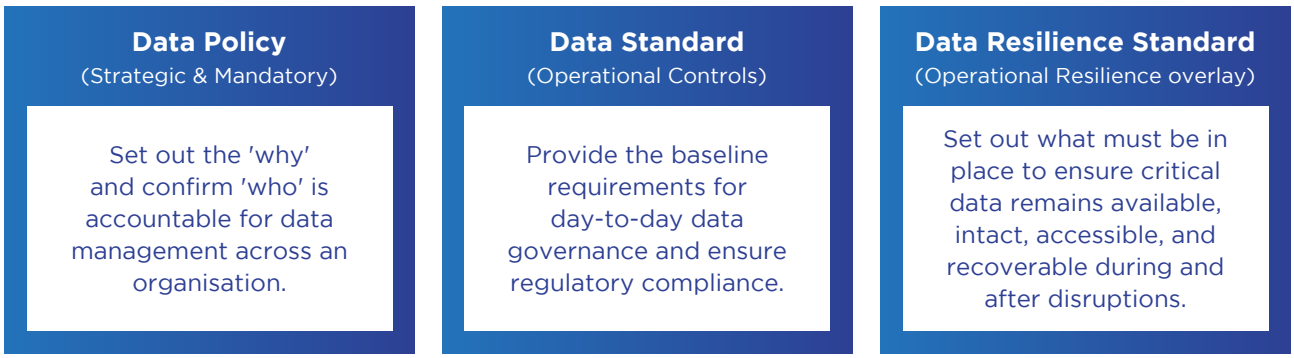
There is an absence of industry-wide agreed definitions for Data Resilience. A consistent and agreed definition helps ensure those striving to embed data resilience by design have a common outcome in mind. A proposed definition would be:

The ability of an organisation to ensure its data remains available, intact, accessible and recoverable during and after disruptions (e.g., cyber-attacks, system failures, accidental deletion, natural disasters and other data related incidents).

Data resilience is foundational for firms to be operationally resilient and demonstrate compliance with regulatory requirements. Regulators such as the UK's PRA and FCA, as well as the EU's DORA framework expect data to be a core component of firm's compliance. In the broader context of operational resilience, firms should ensure there exists the ability to:

- Prevent data loss or corruption by implementing appropriate controls to protect the data from disruption and ensure sufficient redundancy in critical data (i.e., multiple verified and trusted sources of critical data).
- Detect issues early through proactive monitoring and alerting against thresholds which align with an organisation's appetite and impact tolerance.
- Recover data through mechanisms relevant to a firm's data architecture (e.g., through immutable data backup and restore, replication and failover).
- Maintain continuity of the services and functions which are dependent on critical data by identifying critical data dependencies and implementing effective (i.e., tested) contingency arrangements.

Data Resilience requires a joined-up approach, with Data Policy Owners working in partnership with operational resilience teams to achieve a standard set of agreed principles and associated controls which will drive resilience by design across critical data dependencies.



The key principles for data resilience are:

- **Identification:** Critical service critical data dependencies must be identified along with the data sources (i.e., technologies and third parties).
- **Ownership:** Data must have an identified owner – an individual responsible for ensuring appropriate data classification and consistent handling in line with relevant organisational data governance standards.
- **Availability:** Aligned to the critical services which rely upon the data, data must be architected to enable recovery within defined impact tolerances.
- **Integrity:** Mechanisms ought to be in place to validate and monitor data, to detect corruption and enable timely alerting if data corruption occurs.
- **Immutability:** Data must be backed up and immutably protected to ensure the ability to restore data free from unauthorised changes (be it malicious or otherwise).
- **Recoverability:** If primary data dependencies are disrupted (corrupted, unavailable, or no longer usable), protocols must enable end-to-end restoration of data from backups through to business-as-usual (BAU) use in production.
- **Confidentiality:** Critical data must be protected against unauthorised access or disclosure during both business-as-usual and disruption, ensuring customer, counterparty and commercially sensitive information remain secure even while recovery actions are underway.
- **Sovereignty:** Firms must ensure that critical data is stored, processed and recoverable in accordance with applicable jurisdictional requirements, with clear visibility over where data resides and how sovereignty constraints could affect recovery during cross-border or third-party disruptions.

5.3 High quality data is essential for assessing, monitoring and improving operational resilience

To obtain assurance over operational resilience, firms must go beyond narrative and strive for evidence-based assurance, evidence which relies upon data.

Framework component	Data required (examples)	Why data matters	How data supports resilience
Critical services	• Customer outcome data (volumes, customer types, behavioural indicators, etc.) • Market impact data (market significance) • Historical incident and near-miss data (harm patterns) • Complaint and conduct data (indicators of harm) • Financial data (revenue, AUM exposure, liquidity thresholds, etc.)	To identify the critical services which are of most importance, objective evidence is required (that is, more than qualitative judgement). Without data-led decision-making, there is a risk of misidentification or omission of critical services.	Data ensures identification is defensible, consistent and repeatable, reducing subjective bias and ensuring external scrutiny can be withstood.
Impact tolerances	• Historical harm and outage durations • Detriment indicators (e.g., financial loss, complaint spikes, etc.) • Performance data • Customer experience data (e.g., call abandonment rates, waiting times, etc.)	Impact tolerances must reflect real-life harm and true-time sensitivity - this cannot be guessed. Absence of good data can lead to inaccurate tolerances which could result in insufficient resilience capabilities, or lead to mis-prioritised investment.	Data enables firms to set realistic thresholds and enables prioritised investment in protecting critical services outcomes.

Framework component	Data required (examples)	Why data matters	How data supports resilience
Dependency mapping	• Configuration data (systems and technology stack) • Third-party service inventories • Architecture diagrams • Process flows • Ownership data • Monitoring data • Organisational structures and hierarchies	Dependency mapping relies upon complete and accurate reporting of dependencies based upon trusted golden sources for processes, people, facilities, data and third parties. For mappings to be useful they need to be complete and accurate but also maintained to reflect material changes.	Data provides inputs for impact tolerance modelling; enables detection of mapping gaps; and allows for the identification of vulnerabilities (such as single points of failure).
Monitoring impact tolerance breaches	• Service availability • System performance metrics • Data quality indicators • Processing backlogs • Supplier performance data • Control environment monitoring	Ongoing monitoring requires real-time or near-real-time operational data about the health of critical services and their dependencies.	Data helps detect issues before harm is caused; enables predictive modelling and supports timely alerting and escalation.
Scenario testing	• Actual recovery times • Historical incident data • Transaction and processing volumes and values • Dependency data • Supplier recovery data • Data restoration times • Known vulnerabilities	Accurate data on dependencies, volumes, recovery times and actual system behaviour ensures scenario tests are relevant and plausible.	Testing becomes evidence based; reveals hidden dependencies and weak points; and helps validate impact tolerances.
Incident reporting & post-incident analysis	• Incident timestamps • Customer impact records • Tolerance breach data • Incident durations • Drop rates and failed transactions • Root cause classification • Control failures • Supplier incident notifications	Regulators mandate data-driven reporting of incidents which is timely and structured.	Enables the quantification of harm; provides evidence to support the development of remediation plans and can lead to the identification of incident patterns.
Remediation management	• Control metrics • Incident recurrence rates • Reduced recovery times • Backlog resolutions • Supplier performance improvements	Firms are expected to continue to uplift their operational resilience and confirm remediation taken has been effective.	Data confirms whether there are improvements in operational resilience.
Assurance, governance & self-assessment	• Tolerance breach logs • Testing results • Incident logs • Resilience MI • Third-party assurance	For those in scope of UK regulations, self-assessments are mandatory to evidence alignment to regulatory requirements.	Enables board-level awareness and ownership; supports measurability of operational resilience.

5.4 The role of AI

CRO Forum members remain at an early stage in integrating AI into their operational resilience frameworks. While adoption is currently limited, firms consistently recognise AI as a significant future opportunity, with expectations of more widespread use as capabilities and frameworks mature.

Over the coming years, AI has the potential to become central to insurance business strategy, used to help align with Insurance business objectives such as portfolio growth, loss ratio optimisation, customer retention and overall operational efficiency. AI also has the potential to materially strengthen data resilience by improving data quality, identifying anomalies, enabling predictive monitoring of data integrity and accelerating incident detection, impact assessment and recovery decision-making. AI-driven analytics can also enhance resilience testing and post-incident learning by revealing hidden dependencies and patterns that would otherwise remain undetected.

Some high-impact AI and generative AI (GenAI) use cases across the insurance value chain may include:

- Underwriting automation and risk scoring
- Pricing optimisation and actuarial modelling enhancement
- Claims automation and fraud detection
- Customer service virtual assistants and policy servicing
- Document intelligence for policy and claims processing

However, these benefits introduce new resilience considerations: insurers must ensure that AI models, training data and decision outputs remain explainable, trustworthy and resilient to disruption, data corruption or cyber compromise. As reliance on AI-enabled data processing grows, insurers should treat AI systems and supporting data pipelines as critical dependencies, embedding appropriate governance, controls and recoverability so that AI enhances – rather than undermines – operational resilience outcomes.

Reflecting the opportunities and risks posed by AI, the EU AI Act has been established with a phased application from 2026. It is the first regulation of its kind and applies to EU and non-EU organisations where AI outputs are used in the EU. It uses a risk-based approach to set obligations for organisations that develop, sell or use AI systems in the EU, with stricter rules for higher-risk uses.

As regulation increases, this is likely to have a knock-on effect on the operational resilience considerations for organisations.

5.5 Conclusion

Over the next five years, data will increasingly define the insurance sector's ability to demonstrate, deliver and sustain operational resilience. As insurers continue to digitise core activities across underwriting, claims, customer servicing, investment operations and reinsurance, the integrity, availability and recoverability of data will become inseparable from the continuity of critical services and the protection of policyholders.

Loss of data integrity, delayed recovery, or poor data lineage can impair claims settlement, customer outcomes, prudential reporting and legal defensibility long after an incident has been contained. As a result, regulators are increasingly focused not only on whether firms can recover systems, but whether they can restore trusted, complete and usable data within defined impact tolerances.

Looking ahead, several structural trends will heighten this focus. Greater reliance on cloud platforms, third-party data processors, AI-driven decisioning, real-time analytics and automated controls will increase both the scale and concentration of data dependencies. At the same time, supervisory expectations under regimes such as UK operational resilience and EU DORA will continue to evolve toward more data-driven assurance.

To meet these challenges, insurers will need to move beyond reactive data protection measures and embed data resilience by design across critical operations. This includes clear ownership of critical data dependencies, alignment between data governance and operational resilience frameworks and the systematic use of data to identify vulnerabilities, monitor tolerance breaches, test recovery capabilities and demonstrate continuous improvement. Equally, firms must recognise that data quality itself is a risk to resilience: incomplete, stale or inconsistent data can undermine resilience decision-making as effectively as a technology outage.

6. The future threat landscape

6.1 Introduction

Operational resilience has become a defining priority for insurance companies worldwide, driven by a rapidly evolving threat landscape marked by geopolitical instability, technological disruption, climate change and shifting regulatory expectations. The insurance sector, as both a risk absorber and a critical financial infrastructure component, faces mounting pressure to anticipate, withstand and recover from a broad spectrum of shocks. Recent high-profile events, ranging from cyberattacks to climate-driven catastrophes, underscore the interconnectedness of risks and the need for a holistic, forward-looking approach to resilience and have resulted in multi-million-pound losses, operational downtime and significant claims surges. As we look ahead to 2026 and beyond, the focus is increasingly on emerging and future risks, many of which are complex, systemic and global in nature.

6.2 Regulatory and jurisdictional differences

Regulatory and jurisdictional differences are relevant to the threat landscape as they shape where attackers find leverage, how fast disruptions might spread and how effectively an insurer can respond. In a world of accelerating systemic risks, legal fragmentation is itself a threat multiplier – and a vital dimension of operational resilience planning. As set out in the Regulatory Landscape Section, regulatory approaches to operational resilience and emerging risks vary significantly across the UK, Europe, US and globally, creating compliance challenges, operational friction and potential arbitrage opportunities, underscoring the need for robust global risk management frameworks.

6.3 Cyber threats

Cyber risk remains one of the most dynamic and consequential threats to operational resilience. The insurance industry's high-value data, interconnected third-party networks and regulatory scrutiny make it a prime target for cybercriminals and nation-state actors. Recent incidents, such as the Co-op's £206 million loss from a cyberattack, highlight the multifaceted impact of such events: business disruption, data breaches, financial loss, reputational damage and regulatory consequences. The average cost of a major breach now exceeds £4 million per event[1], with sector-wide cyber claims and remediation expenses forecast to double by 2028. These are also increasingly carried out through compromised third-party providers.

The threat landscape is evolving rapidly, with attackers leveraging AI to automate and scale phishing, impersonation and fraud. Ransomware and data extortion are increasingly sophisticated. The shift to cloud and API-driven ecosystems erodes traditional network perimeters and concentrates dependencies, prompting identity-centric, zero-trust architectures and explicit management of cloud concentration risk. Third-party and supply chain dependencies introduce systemic vulnerabilities, as a single vendor compromise can disrupt multiple firms simultaneously. Regulatory frameworks like DORA (EU) and NIS2 are pushing firms toward more transparent governance and rigorous resilience testing, but the pace of threat evolution often outstrips defensive measures.

6.4 Technological threats

Technological innovation is a double-edged sword for insurers. Quantum computing, AI and automation promise transformative benefits in risk modelling, fraud detection and operational efficiency, such as dramatically accelerating risk simulations and enabling unbreakable encryption. At the same time, they introduce new risks, such as the potential for quantum-enabled cyberattacks that could render current cryptographic standards obsolete. Other failures can halt underwriting and claims processing for days, resulting in delayed settlements and reputational harm. The cost of upgrading legacy systems and managing technical debt consumes up to 10% of annual IT budgets for large insurers.

AI-driven automation in claims and underwriting can improve accuracy and speed but also amplifies the risk of systemic errors, algorithmic bias and fraud if not properly governed. The complexity of legacy systems, technical debt and concentrated reliance on a small number of cloud service providers further heighten operational risk. It also highlights the need for manual processes and workarounds as back-ups in case of outages. The sector is also grappling with the challenge of maintaining in-house specialist knowledge. A robust oversight of automated processes to prevent error propagation at scale is key to successfully tackling technological risks.

6.5 Climate threats

Climate change is consistently ranked as the top global risk for insurers, with physical and transition risks converging to create systemic challenges. The frequency and severity of extreme weather events are increasing, global insured losses from natural catastrophes exceeding $120 billion in 2024[2] and forecasts suggesting further increases. Insured losses from natural catastrophes again surpass the USD 100 billion mark in 2025 for the sixth consecutive year according to the Swiss Re Institute. Claims inflation for weather-related events is projected to rise by 20–30% by 2030. The increasing frequency and severity of weather-related events could push many property risks beyond the limit of insurability.

Regulators are responding with enhanced requirements for climate risk assessment, scenario analysis, to demonstrate resilience to climate-related risks, as well as disclosure. However, with data limitations, methodological complexity and the need for forward-looking analysis remain significant hurdles. The insurance sector is also exposed to transition risks as economies decarbonise, with implications for product design, liability and investment portfolios, with significant risks related to customer changing preferences, supply chain disruption and potential of stranded assets. The interconnectedness of climate, cyber and supply chain risks is increasingly recognised, requiring a systems-based approach to resilience.

Affordability and availability pressures are widening the insurance protection gap, making adaptation, resilience and preventive measures a priority for systemic resilience. The European Insurance and Occupational Pensions Authority (EIOPA) has proposed the PROTECT initiative[3], a natural catastrophe risk awareness and prevention solution. PROTECT aims to help property owners reduce vulnerability to extreme weather events, limit potential losses and strengthen Europe's long-term resilience. This consumer-centric tool would provide risk score, tailored prevention measures and insurance-related guidance, empowering citizens to understand exposure and take practical steps. By promoting awareness and preventive action, PROTECT seeks to narrow Europe's insurance protection gap and support climate resilience.

6.6 Sustainability and ESG threats

Sustainability is now central to both regulatory and stakeholder expectations. Insurers are under increasing pressure to integrate ESG (Environmental, Social and Governance) considerations into their risk frameworks, investment strategies, product offerings and operating. The risk of greenwashing, misrepresenting the sustainability of products or investments, is a growing concern, with regulators intensifying scrutiny and requiring more robust disclosures.

Environmental systemic risks, particularly climate change, are recognised by the Emerging Risks Initiative (ERI) Radar 2025 as major drivers of insurer exposure and operational resilience.

A recent industry survey on operational resilience underscores the rising importance of emerging risks. While 87% of respondents consider the evolving threat landscape important or very important, specific ESG-related risks such as climate change -physical risk (6%) and transition risk (2%)- currently rank lower compared to cyber risks (18%) and AI (16%). However, these environmental risks are expected to intensify as regulatory, societal and market pressures accelerate, reinforcing the need for robust ESG integration.

The transition to a low-carbon economy presents both risks and opportunities. The complexity of sustainability reporting, data availability and quality and methodological consistency remains a challenge, particularly as global standards (e.g. ISSB) evolve and diverge from frameworks like TCFD.

Product, underwriting and investment risks: insurers face pressure to develop sustainable products and to exclude or limit coverage for high-ESG-risk sectors (such as coal, oil sands, or controversial weapons). There is growing scrutiny of underwriting practices and the alignment of insurance portfolios with net-zero and broader sustainability commitments. Assets under the ownership and management of insurance companies are similarly expected to align with sustainable investment principles.

Business Continuity Risks: Climate impacts can significantly disrupt day-to-day operations, such as restricting access to offices, systems and other essential resources. Greenwashing Risk: Over-stating or misrepresenting the ESG credentials of products, investments, or operations can lead to regulatory action, litigation and loss of trust.

Social risks (within ESG): Human rights issues in the supply chain, such as modern slavery or poor labour practices, can expose insurers to legal and reputational risks. Community relations and the insurer's role in supporting financial inclusion, disaster recovery and social mobility are increasingly important to stakeholders and regulators. Employee well-being, diversity, equity and inclusion (DEI) initiatives are now seen as core to operational resilience and long-term value creation.

Survey findings show social fragmentation and disorder (3%), highlighting the importance of DEI and community engagement initiatives.

Governance risks: Weak governance structures, lack of board diversity, or insufficient oversight of ESG issues can lead to poor decision-making, regulatory breaches, or ethical lapses. Failures in governance may result in fines, litigation, or reputational harm, especially as regulators and investors increase scrutiny of board accountability and transparency.

In the operational resilience survey, legal and regulatory uncertainty (1%) and collective redress (1%) remain low in perceived impact but could escalate with ESG litigation trends.

ESG Data and Reporting Risks: Inconsistent, incomplete, or inaccurate ESG data can undermine risk assessments, investment decisions and regulatory compliance. The proliferation of ESG reporting frameworks and evolving global standards (such as ISSB, EU CSRD and UK SDR) create complexity and potential for reporting errors or misalignment.

6.7 Geopolitical threats

Geopolitical volatility is a top-tier, cross-cutting driver routed through strategic, market, credit and operational risks; many insurers monitor it via existing frameworks rather than standalone limits, reflecting its transversal nature. The escalation of interstate conflicts, such as Middle East currently experiencing its most severe, open conflict in decades, the ongoing war in Ukraine and rising tensions in the South China Sea, has direct and indirect impacts on insurers. These include disruptions to global supply chains, sanctions regimes and the potential for targeted exclusion from the SWIFT interbank messaging network; exclusion driven by sanctions can disrupt cross-border messaging, complicating claims payments, premium flows, reinsurance settlements and liquidity. Escalating geoeconomic confrontation via sanctions, export controls, currency restrictions and technology restrictions coupled with concentration of technological capabilities in a few countries and firms – raises access and operating-model risks. Supervisors expect insurers to monitor and manage geopolitical risks through their enterprise risk, operational resilience, investment, sanctions and third-party risk management frameworks. The strongest foundations combine both core regulatory requirements that already capture geopolitical drivers, as well as widely used industry guidance on how to operationalize monitoring, scenarios and action triggers. European Insurance and Occupational Pensions Authority (EIOPA) as well as the European Central Bank (ECB) consistently flag geopolitical turmoil, trade fragmentation and cyber escalation as key risk drivers – supervisors expect they are monitored, stressed and integrated into risk appetite and contingency plans. EIOPA

recommends continuing embedding geopolitical risks in insurers' day-to-day business operations and risk assessments, including dependencies on non-EU markets and service providers[4].

State-led and proxy 'grey-zone' campaigns – including cyber-attacks, social media manipulation and other unconventional tactics – are rising. The European Union Agency for Cybersecurity (ENISA) frames digital threats not just as technical issues but as extensions of geopolitical conflict, requiring a holistic, intelligence-driven and collaborative defence strategy . The ENISA Threat Landscape (ETL)[6] report highlights that geopolitical tensions fuel cyber threats, focusing on state-linked campaigns, supply chain attacks, disinformation and AI-enhanced social engineering, demanding intelligence-led responses and cross-functional exercises to counter these hybrid warfare tactics in the digital domain for EU cybersecurity. Insurance companies must also contend with the operational fallout from sanctions, regulatory divergence and the potential for sudden market closures or asset freezes. The sector is increasingly aware that geopolitical shocks can cascade through financial markets, affecting everything from investment portfolios to claims inflation and reinsurance pricing.

6.8 Systemic and interdependent threats

Risks do not remain isolated within a single firm, sector or geography, but instead propagate across multiple domains, amplifying their impact. These threats are characterised by their ability to trigger cascading failures, overwhelm traditional risk controls and create feedback loops that can destabilise entire markets or economies.

Key drivers and examples of these are:

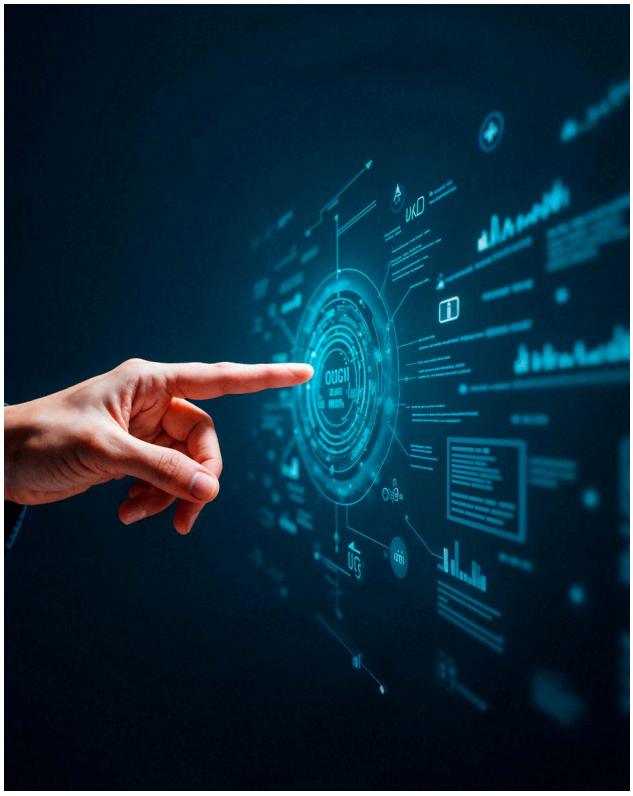
- **Digital interdependence:** The 2025 Co-op cyberattack, which caused widespread operational and supply chain disruption, is a recent example of how digital risks can quickly become systemic.
- **Climate and physical risks:** Climate change is a classic systemic risk, as extreme weather events can affect multiple regions, lines of business and supply chains at once. For insurers, this can lead to correlated claims, capital strain and challenges in risk modelling. The interconnectedness of climate, supply chain and social risks means that a single event (such as a major flood) can have knock-on effects on asset values, customer trust and regulatory scrutiny.
- **Geopolitical and economic shocks** can rapidly propagate through financial systems, affecting investment portfolios, reinsurance markets and operational capabilities. The exclusion of a major economy from the SWIFT system, for example, could disrupt global payment flows and create liquidity crises across borders, causing blocked transactions, asset freezes and liquidity stress that affect claims, premiums and reinsurance settlements.
- **Technological acceleration:** Faster adoption of AI, automation and cloud is creating shared vulnerabilities. With many firms relying on the same AI models and a handful of cloud providers, a single flaw, bad update or cyberattack can ripple across an entire ecosystem all at once. Criminals are also using AI to create convincing scams. Looking ahead, advances in quantum computing could break today's encryption, meaning data stolen now might be readable later.
- **Pandemics and societal shocks:** The COVID-19 pandemic demonstrated how health crises can quickly become systemic, affecting not just health insurance claims but also investment returns, business interruption claims, operational continuity and even the solvency of insurers. Social unrest, demographic shifts, or mass migration can similarly create complex, interconnected challenges.

- **Power:** There is increasing focus on the power consumption of hyperscalers (AWS/Azure among others) as the demand for cloud hosting and AI increases.
- **Reputational risk** damage can arise from a wide range of sources, including operational failures, regulatory breaches, cyber incidents or negative media coverage. For insurers, trust is a core asset, loss of reputation can lead to customer attrition, increased regulatory scrutiny and difficulties in attracting new business or capital. Social media amplify the speed and reach of reputational crises, making rapid and transparent communication essential.
- **Investment risks** are heightened by market volatility, geopolitical instability and the transition to a low-carbon economy. Insurers face challenges from fluctuating asset values, low interest rates and the risk of stranded assets as regulatory and societal pressures shift capital away from certain sectors. The complexity of global markets and the speed of change demand robust investment governance and scenario planning.
- **Geopolitical risk** remains the cross-cutting amplifier across all the key drivers[7], as geopolitical fractures can jeopardise digital supply chains and insurers technological infrastructure[8]. A growing geopolitical concern for the European insurance sector is the dependency on a small number of non-EU cloud service providers, mainly US-based. This concentration creates jurisdictional and extraterritorial risks and stress scenarios that could cause significant service interruption or limit EU insurers' operational continuity.

6.9 Unknown unknowns

The concept of 'unknown unknowns', risks that are not yet on the radar but could have outsized impacts, remains a perennial challenge for operational resilience. Black swan events, such as the COVID-19 pandemic, have demonstrated the limits of traditional risk identification and scenario planning. Building resilience to unknown unknowns requires a culture of continuous learning, investment in horizon scanning and the agility to adapt to unforeseen shocks. Potential future unknowns could include:

- Breakthroughs in quantum computing that suddenly render all current encryption obsolete, leading to widespread data breaches.
- Synthetic biology or bioengineering risks that create new forms of systemic threat (e.g. engineered pandemics). AI-driven market manipulation or autonomous financial systems behaving unpredictably.



6.10 Conclusion

The threat landscape is more complex and interconnected than ever, urging (re)insurers to take a holistic and cross-functional and collaborative approach towards operational resilience. Embedding a coordinated Threat Landscape approach can serve as an integrative and monitoring intelligence benchmark for enhancing an aligned risk and control environment. Emerging and future threats and risks, especially those assessed here of geopolitical, cyber, technological, sustainability and climate - are increasingly systemic, with the potential for cascading impacts across firms, sectors and borders. Disruption may impact both (re)insurers' operational resilience as well as amplify their liability risks with insured businesses seeking coverage for materialised threat events[9]. In parallel, regulatory expectations are rising and evolving quickly and this pace of change demands continuous adaptation. Building true resilience will require not only a culture of agility, collaboration and forward-looking overarching risk intelligence, but robust Governance and controls. Governance is the backbone of operational resilience. It steers, sets guardrails and ensures that security, financial health and crisis readiness all work in harmony. It binds technology, processes and people together. It ensures that resilience is cultural, not just contractual. Governance gives every stakeholder clarity on their role, why it matters and how their actions strengthen the complete ecosystem[10].

7. Governance, culture and capabilities

7.1 Introduction

While organisations increasingly focus on cyber resilience and technical preparedness, operational resilience in the insurance sector is ultimately an enterprise-wide responsibility, critical to the continuity of underwriting, claims management and customer service. It requires clear ownership, behavioural commitment and adaptive capabilities. The CRO Forum survey highlights a disconnect between perceived priorities and foundational enablers: governance and culture remain undervalued despite forming the structural and behavioural conditions for resilient performance and effective policyholder protection. This chapter therefore adopts a holistic view of operational resilience, articulating how governance provides structure and accountability across the insurance value chain, culture drives behaviours and mindsets influencing customer outcomes and capabilities convert both into effective response and recovery. Governance establishes ownership and strategic alignment; culture activates these structures through transparency, learning and early risk detection; and capabilities translate intent into operational performance, particularly in claims handling and outsourced activities. Together, these dimensions embed resilience across the organisation.

7.2 Governance: Framework of operational resilience

The CRO Forum operational resilience survey shows that governance is under-prioritised: only 32% of respondents rate it as "very important," compared with 95% for cyber resilience. However, regulation places governance at the core of resilience. Under the Digital Operational Resilience Act (DORA), boards are explicitly accountable for ICT risk governance, with senior management responsible for defining and overseeing risk tolerance, resources and capabilities. These requirements directly affect insurers' core systems and critical outsourced providers and are reinforced through obligations on incident reporting, metrics, testing and response processes.

Additional requirements related to security awareness, incident communication, resilience testing and third-party risk management embed cultural and capability building mechanisms directly into governance arrangements.[11]

International regulatory principles[12] and supervisory expectations[13] similarly frame resilience as an organisation's ability to withstand, adapt to and recover from disruptions, often through a service centric lens, reinforcing the coordinating role of governance across critical insurance services.

Effective operational resilience relies on strong cross functional collaboration across risk, IT, operations, claims and outsourcing oversight. Clear governance structures – such as dedicated resilience or crisis committees – support consistent decision making, escalation and accountability through defined roles and protocols. Active Board and senior management involvement is critical to embed resilience into strategy, resource allocation and day to day operations. Scenario based stress testing and simulations, tailored to insurance specific events such as claims surges or third-party outages, further strengthen preparedness and decision making under stress.

Viewed in an integrated manner:

- Governance provides structural clarity and accountability across insurance value chains
- Culture promotes openness, trust and shared risk awareness affecting customers outcomes
- Capabilities translate these foundations into adaptive organisational responses

Together, these dimensions form a cohesive system in which governance serves as the structural backbone.

Governance therefore does more than delineate responsibilities: it shapes the organisational conditions under which resilience can take root. By establishing clear ownership, promoting cross-functional coordination and embedding resilience into strategic oversight, governance creates the behavioural and procedural foundations upon which a resilient organisation culture can develop.

7.3 Culture: Embedding resilience into organisational mindset

In insurance, a resilience oriented culture directly influences how employees manage incidents affecting claims processing, customer communication and policyholder trust. It promotes openness, trust and collective responsibility, enabling employees across the organisation – not

only crisis teams – to act proactively in maintaining operational continuity.

Empirical research consistently demonstrates that behavioural and cultural conditions are central to adaptation under stress[14]. Psychological safety enables individuals to raise concerns, share insights and challenge assumptions, while strong trust and communication accelerate recovery during disruptions[15]. These enablers support experimentation, learning and collective sense making – core features of organisational resilience, particularly in customer-facing functions.

Regulatory frameworks increasingly reflect this cultural dimension. DORA embeds behavioural expectations through ICT security training, simulation exercises, structured incident communication and post incident reviews[16]. Similarly, international standards and supervisory guidance (e.g. Basel principles[17], FSB guidance[18] and ISO 22301[19] and ISO 27001[20]) emphasise competence, communication and continuous improvement as essential elements of resilience programmes.

Leadership and the tone from the top

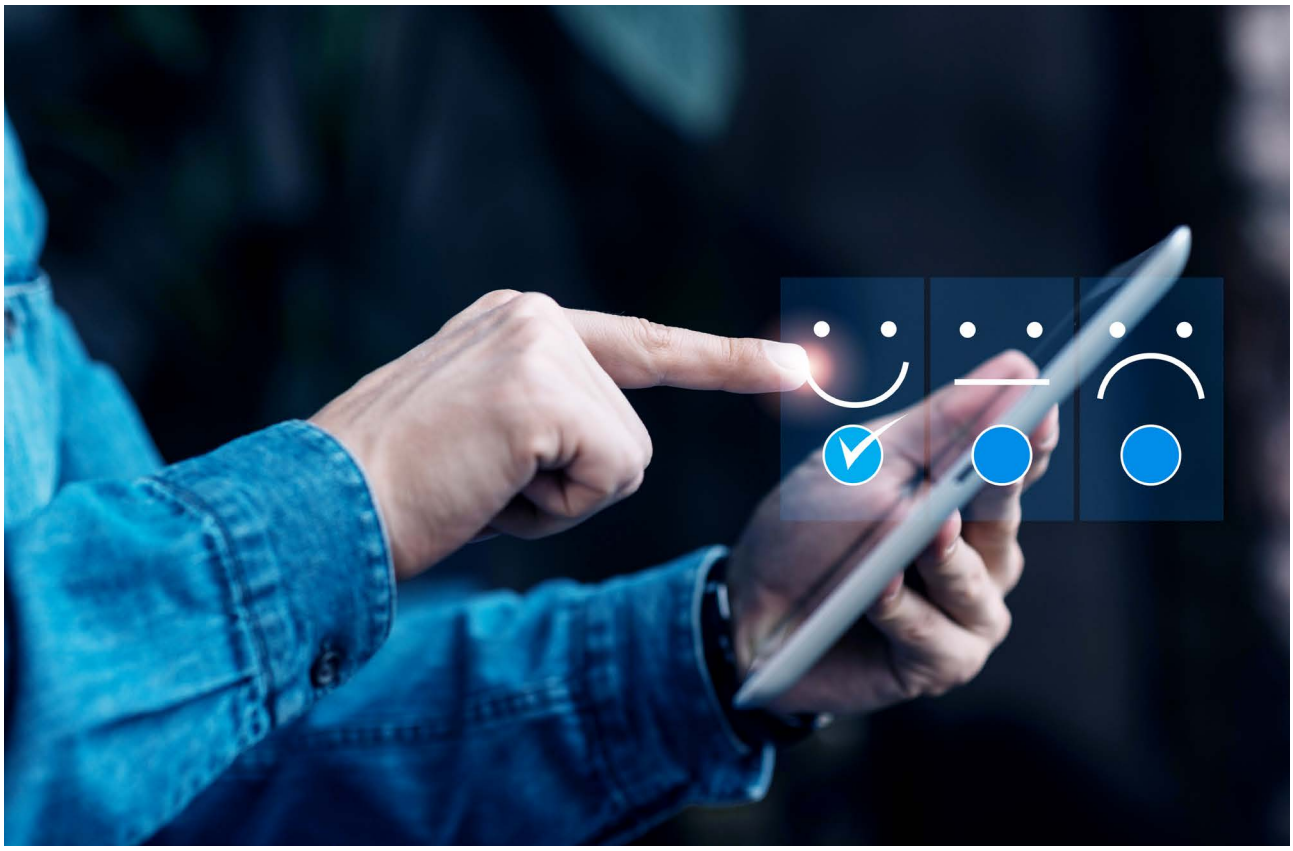
Culture is shaped foremost by leadership. Senior executives must visibly demonstrate resilient behaviours, communicate the strategic relevance of resilience and embed it into decision making processes, particularly where trade offs affect customer outcomes. One illustrative approach is "resilience by design," whereby resilience considerations are integrated into systems and processes from the outset rather than added reactively.

In practice, this approach is often structured around four principles applied across critical resource pillars (people, technology, data, sites and third parties):

- **Modularity** – reducing single points of failure in claims and service delivery
- **Diversity** – ensuring access to alternative resources or providers
- **Redundancy** – maintaining buffers to absorb shocks
- **Adaptability** – enabling resources to be repurposed under stress

Lessons learned

Operational resilience goes beyond absorbing disruption; it depends on learning from incidents. For insurers, where incidents often directly affect customers, effective lessons learned processes are critical. By combining behavioural and procedural aspects – such as communication, escalation, decision making, root cause analysis and control remediation – these processes support continuous improvement and align with DORA's expectations for structured post incident reviews.



Robust frameworks typically include root cause analysis (including third-party risks), cross functional debriefs, transparent communication and tracked remediation actions. Training and scenario based exercises help embed these insights in practice. CRO Forum survey results underline this priority: 15 of 22 respondents identified error culture and lessons learned as key resilience enablers. Treating incidents as learning opportunities rather than blame events strengthens adaptability, psychological safety and ultimately policyholder outcomes.

Awareness, shared practices and continuous improvement

A resilient culture depends on awareness and shared practices. Employees must understand not only procedures, but their purpose and impact on customers. Training, communication and regular simulations embed this understanding and enhance readiness[21], while knowledge exchange across teams and with external partners, including third parties and distributors, prevents resilience insights from remaining siloed.

Despite its importance, culture remains undervalued: only 27% of organisations rate it as "very important," and it is not a stated focus area for 2026–2030 in the survey. This gap underscores the need to translate cultural ambition into tangible capabilities.

7.4 Capabilities: Building resilience skills and resources across functions

Cultural foundations are converted into operational outcomes through capabilities that enable insurers to anticipate, respond to and recover from disruptions. Capabilities transform governance and culture into performance by providing the skills, tools and processes required under stress. Survey results show that this translation is well recognised: 91% of firms use scenario based exercises and 86% conduct live simulations.

Resilience capabilities span risk management, technology, operations and third-party ecosystems and are increasingly viewed as dynamic – the ability to sense, respond and reconfigure resources during disruption[22]. Evidence highlights the role of cognitive flexibility, digital literacy and learning oriented practices. Regular scenario rehearsals improve decision coherence and coordination, demonstrating that resilience depends more on adaptability than on static controls[23] and they improve organisations' ability to learn[24].

These capabilities require strong cross functional coordination. Resilience committees align priorities, monitor metrics and support escalation across risk, IT, operations and compliance. Regulation increasingly mandates this integration, particularly with respect to ICT and critical third-party providers, extending resilience requirements across the insurance supply chain[25].

Capabilities emerge across three interconnected domains:

- **Risk capabilities:** threat identification, scenario analysis and integration of third-party risks in line with governance standards[26].
- **Technology capabilities:** resilience-by-design, redundancy, failover, monitoring and embedded security.
- **Operational capabilities:** business continuity planning, crisis management structures and process mapping to support coherent response, particularly in claims handling.

Building these capabilities is a continuous effort requiring investment, coordination and leadership commitment. When people, processes and technology operate cohesively, organisations are able not only to withstand disruption, but to adapt through it.

7.5 Conclusion

Operational resilience emerges when governance, culture and capabilities reinforce each other. Governance provides structure, culture shapes behaviour and capabilities deliver the response. Survey findings, however, indicate that governance and culture remain underestimated.

(Re)insurers should therefore focus on:

- Elevating governance as a resilience priority: clear accountability, Board oversight and cross-functional alignment across insurance value chains are foundational.
- Strengthening tone from the top: leadership behaviour directly shapes transparency, learning and risk awareness, including conduct risk.
- Reinforcing accountability across the organisation: resilience ownership should extend beyond risk and IT to business and claims teams, reflecting customer and regulatory expectations.
- Integrating people and process learning: a holistic lessons learned discipline accelerates improvement and reduces the recurrence of systemic weaknesses that affect customers.

8. Conclusion – What is the 2030 Insurance sector vision?

8.1 Operational resilience: The next five years, shifting from compliance to strategic capability

Operational disruption is no longer exceptional – it is the operating environment. Cyber threats, geopolitical instability, climate events, technology concentration and deep reliance on third-party ecosystems are reshaping how financial institutions must manage resilience. At the same time, the sector's growing interconnectivity amplifies the severity and reach of disruption.

Over the past five years, global regulations have driven significant advancement. However, the next phase requires a shift: from regulatory compliance to strategic, system wide resilience built into how institutions design, operate and govern their businesses.

There are four strategic outcomes that should define the industry's evolution over the next five years:

1. Shift from compliance to protecting the Minimum Viable Business (MVB)

Regulatory frameworks rightly anchor resilience in critical services. However, to remain viable in prolonged or severe disruption, institutions must evolve this into protecting the Minimum Viable Business (MVB) – the smallest version of the enterprise capable of:

- serving customers' core needs
- meeting regulatory and legal expectations across jurisdictions
- preserving market integrity
- maintaining investor and shareholder confidence

MVB thinking reframes resilience from a regulatory exercise to continuous service assurance, covering end to end processes, dependencies and decision making pathways.

Key priorities

- Define and map the institution's MVB and its critical services
- Identify critical dependencies across people, technology, facilities and third parties
- Set operational tolerances that reflect customer, regulatory and financial stability outcomes
- Embed resilience metrics in enterprise risk reporting
- Move from periodic assessments to ongoing monitoring and evidence based assurance

Institutions should be able to demonstrate – through testing and real life scenarios – that they can operate within MVB tolerances during severe disruption.

2. Drive resilience by design across technology, operations and third parties

Resilience must be engineered into the firm – not bolted on through contingency plans. This requires embedding resilience in:

Technology architecture

- Simplified and modernised platforms
- Resilient cloud and hybrid architectures
- Automated recovery and failover models
- Zero trust security
- Continuous resilience testing

Leading organisations accept that systems fail; they design so that failure does not become disruption.

Business and operational design

Technology is only one source of fragility. Resilience also depends on:

- workforce availability and succession
- crisis management capability
- operational surge capacity
- location and facilities resilience
- outsourcing continuity

Sectors such as insurance need additional resilience to manage large scale claims events during catastrophic incidents.

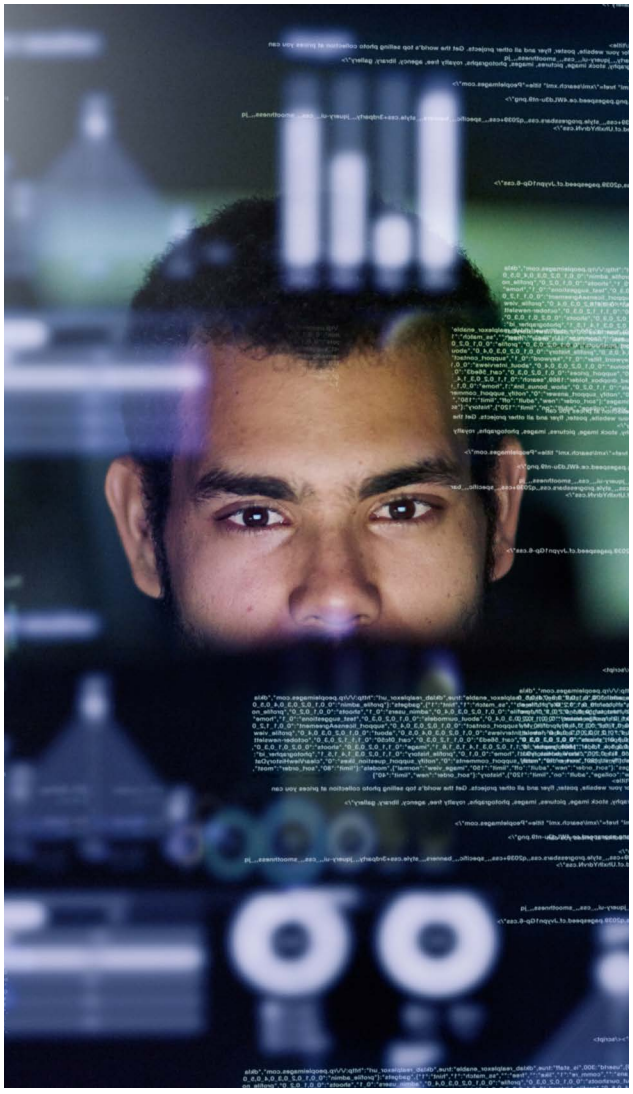
Third-party and ecosystem risk

The industry now depends heavily on a small number of global providers – including cloud platforms, telecommunications networks and core software suppliers. This creates systemic concentration risk beyond the control of any one institution.

Institutions must shift from supplier level oversight to ecosystem level risk management:

- identify cross industry concentrations and single points of failure
- carry out enhanced due diligence for critical suppliers
- test and maintain credible exit and substitution strategies
- include top suppliers in resilience exercises

This challenge cannot be addressed by firms alone and requires structured collaboration with industry bodies and supervisors.



3. Strengthen Board and executive accountability with better MI and real scenario testing

Operational resilience is ultimately a governance responsibility. Boards and executives need clearer accountability, more insightful reporting and greater involvement in resilience decision-making.

Board and executive expectations

- Approve operational tolerances for IBS and MVB
- Receive regular, meaningful resilience MI – not technical reports
- Participate in severe but plausible scenario exercises
- Challenge management on ecosystem and systemic dependencies

Institutions must also move away from theoretical scenarios and incorporate real-world events – cyber incidents, geopolitical instability, supply chain shocks and financial sector disruptions – to test preparedness and decision making under pressure.

4. Expand and formalise cross industry collaboration

Systemic risks cannot be solved institution by institution. Increased interdependence between firms, markets and technology providers means the next phase of resilience must be collaborative, not isolated.

Sector wide resilience testing

The industry should adopt joint exercises involving:

- major cyber attacks
- cloud or telecom failures
- payment infrastructure disruptions
- simultaneous cross firm incidents
- failure of a sector-critical third-party

These exercises should include financial institutions, regulators, sector infrastructure providers, critical technology suppliers and bodies such as the CRO Forum. Over time, they should evolve into sector level resilience stress tests.

Enhanced information sharing

Stronger frameworks are needed for:

- real time threat intelligence
- operational incident reporting
- systemic vulnerability identification

This requires resolving challenges around legal barriers, reputational risk and inconsistent reporting.

Collaboration with critical technology providers

Regimes such as the UK Critical Third Parties framework and EU DORA oversight are important steps. Firms should leverage them to build:

- more transparent risk dialogue
- joint testing programmes
- coordinated outage response protocols

8.2 What is the role of the chief risk officer?

CROs will be central to shaping this evolution. Over the next five years, CROs should focus on:

Strategic leadership

- Integrate operational resilience into enterprise-wide risk strategy
- Establish clear and measurable resilience metrics
- Promote resilient by design across technology, operations and third-party management

Capability development

- Mandate severe but plausible scenario testing incorporating real world events
- Build cross-functional resilience teams (risk, operations, technology and crisis management)
- Strengthen oversight of third-party and ecosystem-level risks

Industry engagement

- Participate in sector-wide simulations
- Promote information sharing initiatives
- Engage proactively with regulators on systemic resilience issues

8.3 Conclusion

Operational resilience is becoming a defining capability for financial institutions. The organisations that will thrive are those that:

- shift from compliance to protecting their Minimum Viable Business (MVB)
- manage ecosystem and concentration risks, not just individual suppliers
- design technology and operations to fail safely
- equip boards and executives with the insight and accountability to lead during crises
- collaborate across the sector to address systemic risks

Resilience is no longer about regulations – it is about maintaining trust in the financial system in an era where disruption is constant and inevitable.

Appendix A

Glossary of key terms

Term	Definition
BCM (Business Continuity Management)	A management discipline that identifies critical services and dependencies and establishes plans and capabilities to maintain and recover them during disruption.
CBEST	A UK framework for intelligence-led penetration testing, used to assess cyber resilience against sophisticated threat actors (aligned to the TLPT concept).
CNI (Critical National Infrastructure)	Nationally important systems and assets (e.g., energy, telecoms) whose disruption would have significant societal or economic impact.
Concentration risk	Risk arising from over-reliance on a single supplier, technology, geographic region, or shared provider, creating potential single points of failure and systemic vulnerability.
Critical Third-party (CTP)	A third-party provider designated by regulators due to systemic importance.
Critical services / important business services	Services delivered by the firm where disruption could cause harm to customers/policyholders, threaten market integrity, or impact the firm's safety and soundness.
Cyber resilience	The ability to protect, detect, respond to and recover from cyber threats while maintaining critical services and protecting confidentiality, integrity and availability.
Data resilience	The availability, integrity and recoverability of critical data during and after disruption.
Dependency mapping	The process of identifying and documenting the people, processes, technology, data, facilities and third parties that support delivery of a critical service end-to-end.
DR (Disaster Recovery)	Capabilities and plans to restore technology services and data following an outage or disruptive event.
DORA (Digital Operational Resilience Act)	EU regulation that sets requirements for ICT risk management, incident reporting, resilience testing, third-party risk management and information sharing for financial entities.
E2E (End-to-End) testing	Testing that assesses whether a critical service can be delivered across the full chain of dependencies (people, process, technology, data and third parties) within defined tolerances.
Exit strategy	A planned approach for transitioning away from a third-party (or substituting a service) to maintain continuity, including contractual, operational, data and technical considerations.
FCA (Financial Conduct Authority)	UK conduct regulator for financial services firms, including operational resilience requirements for firms in scope.
FMI (Financial Market Infrastructure)	Systems that support clearing, settlement and payments (e.g., payment systems, central counterparties), on which insurers may depend for transactions and cash flows.
Horizon scanning	A structured process to identify emerging threats and trends that could affect the firm's resilience, used to inform scenario design and preparedness.
Hyperscaler cloud provider	A very large cloud service provider offering global-scale infrastructure and services (e.g., compute, storage, networking), often creating concentration and systemic dependency risks.
IAIS (International Association of Insurance Supervisors)	Global standard-setting body for the insurance sector, producing supervisory guidance including on operational resilience.

Term	Definition
ICT (Information and Communication Technology)	Technology assets and services used to process, store and transmit information, including applications, infrastructure, networks and related third-party services.
Impact tolerance	The maximum tolerable level of disruption to a critical service.
Incident management	Processes and roles for detecting, triaging, responding to and recovering from operational and technology incidents, including escalation and communications.
Intolerable harm	A level of harm to customers, clients, policyholders and markets from which cannot be easily recovered in the medium to long term, used to set impact tolerances.
Minimum Viable Business (MVB)	The smallest set of services, resources and processes required for the firm to remain viable and meet core customer, regulatory and market integrity outcomes during severe disruption.
MTD (Maximum Tolerable Downtime)	The longest period a service may be unavailable without causing intolerable harm.
Nth-party risk	Risks originating from a third-party's own suppliers and dependencies.
NIS2	EU directive strengthening cybersecurity and incident reporting obligations for essential and important entities, relevant to the broader resilience regulatory environment.
Operational resilience	The ability of an organisation to prevent, detect, respond to, recover and learn from disruption while continuing to deliver critical services.
Outsourcing / Third-Party Risk Management (TPRM)	A framework of policies, processes and controls to identify, assess, manage and monitor risks across the lifecycle of third-party relationships, including resilience and concentration risk.
PRA (Prudential Regulation Authority)	UK prudential regulator for banks, insurers and major investment firms, including operational resilience requirements for firms in scope.
Recovery Point Objective (RPO)	Maximum acceptable amount of data loss measured in time (i.e., the point in time to which data must be recoverable after an incident).
Recovery Time Objective (RTO)	Target time to restore a service, system, or process after disruption to an acceptable level of operation.
Resilience-by-design	Designing processes, services, data and technology so they can fail safely and recover within tolerances, rather than relying solely on contingency planning.
Scenario testing	Exercises using severe but plausible events to validate operational resilience capabilities.
Severe but plausible	A scenario design standard requiring events to be extreme enough to test meaningful resilience, while remaining credible given the firm's context and threat environment.
SIMEX	The Bank of England, in partnership with UK Finance, the financial sector and the other UK financial authorities (HM Treasury and the Financial Conduct Authority), undertake bi-annually UK market wide simulation exercises - SIMEX. The simulations set out to exercise the UK financial sector's ability to respond to a major infrastructure failure that would be expected to have systemic catastrophic impact across the sector. SIMEX has been developed and delivered by the Cross Market Operational Resilience Group (CMORG), a strategic partnership between the financial authorities, UK Finance and industry, established by the Bank of England in 2015.
Single point of failure	A component, dependency, or process that, if it fails, could cause disruption to a critical service due to lack of redundancy or effective workaround.

SRTO (Service Recovery Time Objective)	A target time for restoring a critical service to an acceptable level following disruption (term used in some supervisory guidance, e.g., MAS).
Systemic risk	Risk that a disruption could propagate beyond a single firm and impact the wider financial system, markets, or economy, often via shared dependencies and interconnections.
Technology resilience	The ability of technology services (applications, infrastructure, networks) to withstand disruption and recover within defined objectives, including redundancy, graceful degradation and failover.
Threat-Led Penetration Testing (TLPT)	Regulatory testing that simulates real world threat actors.

Endnotes

[1] IBM Report: UK Sees Drop in Breach Costs as AI Speeds Detection

[2] Global nat cat losses soar to $120 billion in 2024, Munich Re reports | Reinsurance Business

[3] Its use would enhance awareness of emerging risks and support better outcomes for individuals, communities and the insurance sector. EIOPA website (link).

[4] The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) today issued their Autumn 2025 Joint Committee Report on risks and vulnerabilities in the EU financial system. The Report highlights how tensions in global trade and the global security architecture have deepened geopolitical uncertainties. The authorities call for increased vigilance and urge financial entities to maintain adequate provisions in today's tense and unpredictable environment. 19 September 2025, EIOPA website (link).

[5] ENISA Threat Landscape: Finance Sector, 21 February, 2025, ENISA website (link).

[6] ENISA Threat Landscape 2025, 1 October 2025, ENISA website (link).

[7] World Economic Forum, Global Cybersecurity Outlook, January 2026. In an increasingly fragmented global environment – marked by conflicts, geoeconomic tensions, trade wars, sanctions and growing technological competition – geopolitics has become a defining force shaping cybersecurity. Survey data reveals that, although the percentage of organizations changing their cybersecurity strategy due to geopolitics has declined from 93% in 2023 to 66% in 2026, geopolitics remains the top factor influencing overall cyber risk mitigation strategies. This suggests that the initial wave of adaptations following the geopolitical turmoil that dominated the headlines in 2022 and 2023 has passed, and that geopolitical risk is now a major factor shaping cyber defence.

[8] Central Bank of Ireland, Regulatory & Supervisory Outlook, February 2026. *Geopolitical fractures can jeopardise digital supply chains, including the security and continuity of access to AI models and the technological infrastructure used in financial services. (Re)insurers are operating in an increasingly challenging and volatile macroeconomic and geopolitical environment.*

[9] International Association of Insurance Supervisors, IAIS, Global Insurance Market Report, December 2025. Underwriting risks: *[...] geopolitical tensions have contributed to a rise in cybercrime, further increasing insurers' exposure to operational risks, as well as liability risks as businesses seek coverage for cyber incidents and data breaches*.

[10] 9th Conference on Global Insurance Supervision, Building Resilience in a Risk-Driven World. Frankfurt, 3 September 2025. Session Operational resilience: just a question of governance? Moderated by Marc Andries, DORA Joint Oversight Director appointed by the three European Supervisory Authorities (ESAs) European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA).

[11] Digital Operational Resilience Act (DORA) — consolidated reference to Art. 5,17,18

[12] Basel Committee on Banking Supervision, Principles for Operational Resilience (2021)

[13] UK FCA/PRA operational resilience regime

[14] Bahadurzada et al. (2024)

[15] Williams et al. (2023)

[16] Digital Operational Resilience Act (DORA) — consolidated reference to Art. 5(1)(g), 10, 11, 14

[17] Basel Committee on Banking Supervision, Principles for Operational Resilience (2021)

[18] Financial Stability Board (FSB), guidance on operational resilience (2022)

[19] ISO 22301 — Security and resilience — Business continuity management systems

[20] ISO 27001 — Information security management systems

[21] Digital Operational Resilience Act (DORA) — consolidated reference to Art. 10,11

[22] Khan (2024)

[23] MIT Sloan Management Review (2024)

[24] Schroeder et al. (2025)

[25] Digital Operational Resilience Act (DORA), Art. 28–30; also Bank of England SS6/24 (Operational resilience: Critical third parties)

[26] See Footnote 23

Disclaimer

The CRO Forum is supported by a Secretariat
that is run by KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands

www.thecroforum.org