KPMG

Operational resilience

Building a competitive advantage

KPMG Middle East

November 2025

Contents

Introduction

Firms have long been operating in an environment of interconnected and overlapping crisis. To survive and thrive, the most valuable currency for firms is the trust of their stakeholders - be it regulators, investors, customers, suppliers, or employees.

The question firms need to ask themselves is not "if" but "when" will the next crisis strike? And when it does – will they be prepared to remain worthy of their stakeholders' trust?

Firms have a tremendous opportunity to build this trustworthiness by demonstrating their ability to remain operationally resilient and bounce back stronger through any crisis or disruption.

Firms that recognise this opportunity and invest in building a strategic operational resilience capability will gain a significant competitive advantage enabling them to capitalise on opportunities where their competitors may be less prepared.

It's a very exciting time to be sat at the heart of operational resilience, and the next few years promise to inculcate a feeling of permanent dynamism. Now is the time to invest in and prepare for the future.

Beyond recovery to mitigating external harm

Financial services firms have long engaged in various forms of testing to ensure business continuity management (BCM). Whilst (BCM), IT disaster recovery (ITDR), and crisis management testing all provide valuable insights into a firm's internal recoverability, the emergence of Operational Resilience regulations across a number of jurisdictions highlights the need for a complementary approach to traditional BC and ITDR exercises.

Firms must now consider how they will conduct scenario testing to mitigate external harm, with a specific focus on the potential disruption caused to customers and wider market from severe but plausible scenarios. Moreover, many firms have received feedback that they must make their scenario testing more complex and severe, which necessitates the requirement for them to move from traditional desktop testing to live testing.

We have found that this cultural shift requires tooling to facilitate focused testing. Platforms such as Fusion's scenario testing capability can help firms leverage data science and artificial intelligence (AI) to identify potential areas of concern, prioritise these, and conduct targeted testing which has been informed by data-driven insights.

At the time of writing, specific financial services operational resilience regulation has not been formally released by the Central Bank of the UAE (CBUAE), however, this is expected and many organisations are rightly preparing for it.

Actionable approaches to build and operationalise a sustainable Operational Resilience capability:

1. Accountability and clear tone from the top

Boards need to take ultimate accountability for resilience as a strategic business imperative. This accountability shouldn't be diluted by delegation to complex risk and governance structures. Leaders need to be vocal and empower the organisation to take resilience-led decisions and demand metrics that are forward looking e.g. recovery rate of services vis-à-vis competition.

2. A mindset shift that puts resilience at the heart of everything

Nothing changes until mindsets change. Boards and C-suite executives need to drive this narrative into the heart of the organisation. They need to incentivise bringing together complimentary capabilities like operational risk management, business continuity management, IT and cyber risk management, third party risk management etc. to achieve the resilience imperative. The traditional inward facing view of the organisation is no longer fit for purpose and needs to pivot to a customer-led service delivery view. The executive focus also needs to put resilience by design at the centre of their strategic business decision making process.

3. Pivot from a cost narrative to a return-on-investment narrative

The cost of not being resilient is simple – you may no longer be in business. This hard-hitting reality is what needs coming to terms with. Instead of thinking how much a resilience initiative will cost, the pivot needs to be how much return this investment will generate in the form of increased market share and client retention by making services more reliable.

From internal focus to mitigating external harm

While existing testing methodologies predominantly focus on internal recovery and ensuring a firm's ability to restore applications and processes within its risk appetite, they may not adequately address the need to understand whether a service can be recovered within impact tolerance and the potential impact of a disruption on external stakeholders, including customers and the broader market. Operational resilience introduces a new lens, emphasising the need to mitigate external harm caused by operational disruptions. This shift requires a new type of testing that goes beyond assessing internal recoverability.

Scenario testing

Scenario testing in the context of operational resilience focuses primarily on important business services (IBS) and involves the development of scenarios that could severely disrupt the provision of these services to customers. The goal is to understand how a business will respond to such disruptions and what workarounds/ substitutes could be deployed to mitigate the impact on external end users. This also involves assessing the effectiveness of communication strategies and any third-party support mechanisms.

Enhancing testing approaches

Firms have started to increase their scenario testing activities in response to operational resilience regulations, however, in the round, many are still conducting desktop, simulation-based testing. While desktop testing can provide valuable insights, regulators emphasise that this type of testing, too often, relies on SME knowledge and does not provide the data-driven insights required to provide assurance to senior leadership and the Board of the overall resilience posture of an IBS. Many firms are now considering how they can transition to live testing to further assess the response and recovery capabilities of their IBS.

Live testing does not mean shutting down a complete system. Instead, it involves pushing a small number of cases through the workaround process to confirm its efficacy and identify any potential vulnerabilities that may arise when using the live capability, which would not necessarily be identified through desktop testing.

> **Operational resilience introduces a new lens, emphasising the need to mitigate external harm caused by operational disruptions. This shift requires a new type of testing that goes beyond internal recoverability and focuses on mitigating harm to customers.**

Unlocking the power of third-party risk management

In today's interconnected business environment, organisations rely heavily on an interconnected web of third-party vendors for critical operations. This reliance amplifies the complexity of third-part risk management (TPRM) and places significant pressure on companies to manage these risks effectively amidst stringent regulatory requirements and the potential for significant operational disruptions.

The failure of third-party vendors can lead to interruptions in essential services, further increasing the need for robust TPRM frameworks to ensure both compliance and operational resilience.

In the UAE, many non-financial services organisations who are implementing operational resilience rely heavily on their supply chain. Value chain mapping is a fundamental operational resilience requirement for many of these firms.

However, many firms struggle with fragmented and siloed risk data spread across various departments and systems. Key information is often dispersed among procurement platforms, risk assessment tools, governance, risk, and compliance (GRC) systems, and numerous spreadsheets and questionnaires stored in disparate files and folders.

This data fragmentation leads to several critical challenges:

Limited risk visibility	Without a unified view of third-party data, organisations find it difficult to assess their overall risk exposure accurately. This lack of visibility hampers their ability to identify high-risk vendors and areas of concentration risk, leaving them vulnerable to unforeseen disruptions.
Regulatory compliance risks	Disjointed data management can result in incomplete or inaccurate reporting to regulators. Firms may struggle to meet obligations under regulations on outsourcing and third-party risk management (e.g. PRA's Supervisory Statement SS2/21 in the UK), potentially leading to compliance breaches and financial penalties.
Inefficient decision-making	Decision-makers lack timely access to critical insights, making it challenging to prioritise oversight activities or respond swiftly to emerging risks. This inefficiency can hinder the organisation's agility and competitive edge.

Focus areas

Many organisations face challenges in effectively managing their TPRM data and reporting. Companies are seeking to overcome these hurdles by focusing on two key areas:

- **Integration of TPRM data sources**: By combining data from various sources — procurement systems, GRC platforms, risk assessment tools, and even spreadsheets — organisations can create a comprehensive view of their third-party risk landscape. This integration enables more accurate insights and better visibility into the overall risk profile.
- **Value chain and dependency mapping:** Understanding the value chain that supports end-to-end important business services is critical to many organisations. The impact of outages along the value chain may have detrimental effects on a market heavily dependent on trade into and out of the UAE. Multiple major UAE-based organisations including oil and gas, FMCG, transport, and tourism need to map and build resilience into their supply chains.
- **Self-service reporting**: To reduce the operational burden of manual data requests and enable real-time insights, organisations are moving towards self-service reporting. This allows stakeholders to access live metrics on third-party risks, improving the efficiency and effectiveness of risk management processes.

Bridging the gap

We have worked with multiple organisations to help them bridge their data gaps and provide more reliable and actionable TPRM insights. By blending our third-party risk and data analytics expertise, we have defined key elements demonstrating the 'art of the possible':

- **Key third party risk metrics** that are required to enable effective decision-making of various aspects of third-party risk.
- **An extended TPRM data model** to capture data from the underlying siloed systems and provide an MI and Analytics repository, enabling regulatory reporting, risk management and decision-making
- **Persona-based illustrative dashboards** showcasing a tangible and achievable target for organisation to strive for when realising their TPRM data strategies.

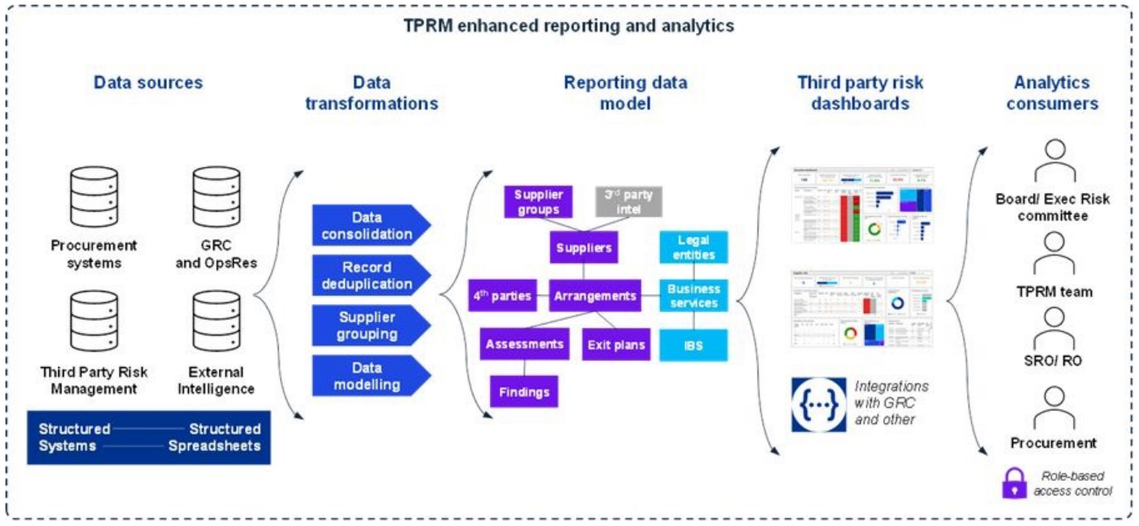
A high-level data flow enabling this is presented below:

Potential actions

These are some no-regret actions that companies can take to get started on combining third-party risk data and creating reporting that would help to improve risk governance and decision making.

1. **Articulate and prioritise third-party risk reporting requirements**: Create reporting wireframes to validate key metrics and secure buy-in, then prioritise and document high-priority metrics along with their relevant data sources.
2. **Understand key data fields and data quality**: Identify data fields needed to meet critical reporting requirements as well as any gaps in existing data. Identify how key data sets will be combined together, particularly for datasets from disparate systems.
3. **Run a limited pilot to build foundations and get quick wins**: Establish a foundational data model that can be expanded with additional data and metrics. Share early successes with stakeholders to gain support for further improvements.

Given the typical size and complexity of TPRM data, we find that this iterative approach helps to gradually build a more robust data framework and governance, while allowing an opportunity to discover the requirements and demonstrate value early on.



Resilience by design

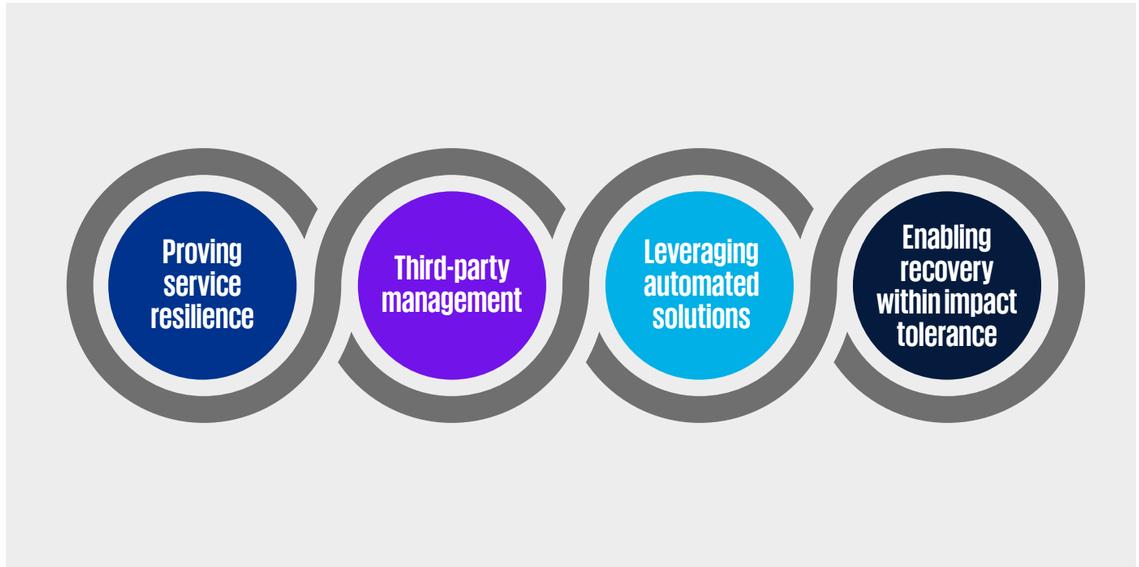
Resilience by design is an enduring methodology carried over from the technology resilience by design concept that can help your organisation manage resilience gaps in the face of change and defend against emerging threats. In today's world, operational resilience is more critical than ever, with cyber-attacks, pandemics, and extreme weather events adding to ever-increasing challenges.

By adopting a principles-led, risk-based approach to managing change to IBS, organisations can ensure that they continue to be well-prepared to weather any storm. Resilience by design is a component part of an organisation's approach and complements the operating model, tooling, and people elements by supporting the resilience lifecycle and change processes.

What is resilience by design?

Resilience by design is a set of tools that can help you achieve this goal. It involves implementing comprehensive resilience principles into your organisation's change management processes, ensuring comprehensive coverage across all scenarios and pillars of resilience, including people, property, technology, third-party, and data/security. Resilience principles are intended as a guide for change practitioners to enable them to enhance an IBS and prove its resilience through leveraging automated solutions, whilst ensuring appropriate oversight and approval to ensure the recovery of the service within impact tolerance.

By developing and implementing these principles iteratively, you can ensure that resilience by design is embedded within your business-as-usual organisational change processes, without significantly increasing cost, resource, or timelines for future changes.



Implementing resilience by design

Before implementing resilience by design, it's important to confirm the scope of the principles. You'll need to consider the cost, time, and resource implications of increasing the resilience requirements for your services through change activity and determine whether you want to implement the approach for IBS only or to include other business services and systems. Regardless of your decision, you'll need to assess your principles against severe but plausible scenarios, known vulnerabilities, and historic incidents to ensure that they provide appropriate coverage. This assessment will help develop requirements that will underpin the overarching principles for change practitioners to use as a handrail.

To ensure that resilience by design is successful, you'll need to confirm that there are appropriate checkpoints and controls in your organisation's business-as-usual change management process. By doing so, you can monitor the adoption of and compliance with the resilience by design principles, identify and remediate areas of exposure through non-compliance, and address thematic resilience issues if recurring resilience gaps are identified. It is important to extend the adoption of resilience by design to your third-party providers, requiring compliance through contractual obligations or considering alternative mitigation.

A change of mindset

Implementing resilience by design is a transformative process that surpasses simple changes to structure, policy and processes. It requires a fundamental shift in the organisation's culture and mindset. As resilience by design focuses on proactively anticipating and adapting to future challenges, instead of reacting to them, the board and senior executives must set the tone from the top with their commitment to the required cultural change. Through championing resilience by design the board and senior executives can create a ripple through the organisation which empowers and motivates individual colleagues to seek opportunities to improve resilience and find innovative solutions.

Ultimately, the goal of resilience by design is to ensure that your organisation remains operationally resilient, no matter how much changes or what challenges come your way. By continuously scanning the horizon for emerging threats, gathering strong market intelligence, and updating your resilience principles accordingly, you can ensure that you are well positioned to recover your IBS within impact tolerance in the face of any disruptions. It's important to achieve operational resilience, but it's essential to maintain it. So why not take the first step towards implementing resilience by design in your organisation today?

Resilience to climate change

The impact of climate change on infrastructure

In recent years, the world has seen variable weather patterns, with some cold regions experiencing unusually warm summers while other warmer countries have faced colder temperatures. The heavy rainfall in the UAE in April 2024 was a case in point. Climate change exacerbates extreme events, pushing infrastructure outside of its operating tolerances. Almost all organisations own, manage, or rely upon infrastructure systems for transport, energy, water, accommodation, and communications. Infrastructure owners face increasing pressure to maintain ageing infrastructure while meeting growing customer demands in a changing climate, and within challenging financial pressures.

Climate change and extreme weather events pose a risk to essential services, impacting public health and the economy. With increasingly costly maintenance and adaptation of infrastructure, asset owners must explore low-cost options for mitigating the impacts of climate events on customers. For example, proactively managing customer journeys via weather alerts for expected disruptions in advance. Changing work habits and technological advancements such as homeworking, have reduced the impact of infrastructure failure.

The effects of climate change and the global government commitments to achieve net zero place increasing strain on infrastructure. Asset owners and customers face two types of climate risks:

1. **Physical risks** associated with climate change, such as extreme temperatures, strong sandstorms and higher rainfall could accelerate infrastructure degradation and failure.
2. **Transition risks**, the shift to a net zero economy affects existing business models as demand for products and services evolves.

Infrastructure owners have already experienced the impacts of climate change

In 2024, the UAE experienced exceptional rainfall that required a strong and well-coordinated national response. The actions taken by the UAE government demonstrate the country's effective crisis management capabilities and commitment to pubic safety.

This highlights the need to focus on the interconnected nature of our infrastructure systems, their vulnerabilities, and the need for effective risk management and resilience in the face of climate change.

Organisations must prioritise infrastructure resilience to mitigate such crises, protecting lives and safeguarding business continuity. to mitigate such crises, protecting lives and safeguarding business continuity.

The impact on organisations

The repercussions of infrastructure

systems failure due to climate events are profound for organisations. The overall standing of the organisation is weakened by monetary penalties, impaired market perception and investor/public confidence.

Organisations, particularly those reliant on critical infrastructure, must recognise the urgency of proactive measures. By comprehensively assessing risks, strategically investing in modernisation, and empowering corporate risk functions, organisations can navigate the challenges posed by climate change.

A path forward

Addressing climate change demands a proactive and strategic approach focused on understanding physical and transition risks. Focus should be on the cost-effectiveness of early action.

However, with finite resources, strategic funding allocation is needed to ensure that solutions are provided without compromising customer needs or the financial position of infrastructure owners. This requires an approach that effectively manages risks without gold plating and future proofing every solution.

Corporate risk functions are critical in addressing climate change; responsible for assessing, managing, and mitigating physical and transaction risks, whilst applying systems thinking. By reconsidering risk management strategies in the context of infrastructure resilience, organisations can proactively manage climate-related impacts and adapt to the transition to a net zero economy.

Strategies for infrastructure resilience

Organisations should adopt a risk-based mindset, accepting the need for transformation, developing a deeper understanding of climate risks and establish an appetite to tolerate these risks. This provides a basis for decision making. We have identified the following steps for achieving asset and infrastructure resilience, which can be completed individually or together to enhance your risk capabilities and ability to predict and respond to the impacts of climate change.

Comprehensive risk assessment	Strategic investment in modernisation and adaptation	Empower corporate risk functions and integrate climate resilience
Undertake a thorough risk assessment to identify and prioritise physical and transition risks associated with climate change. The assessment must consider the criticality of each asset in maintaining the levels of service expected by customers. This involves creating a heatmap of vulnerable infrastructure by analysing regional climate patterns and modelling potential future scenarios. The insights form the basis for targeted and effective resilience strategies.	Allocate resources for the modernisation and adaptation of critical infrastructure assets, prioritising those identified as vulnerable and/or critical assets. Strategic investments can help long-term sustainability and resilience against climate-related challenges. However, continuous risk management is required to proactively identify when climate change may push assets out of their safe operating tolerances. Asset owners can also consider proactive customer management strategies during climate-events, for example, using alerts to promote remote working during storms.	Elevate the importance of risk appetite and tolerance on the executive board's agenda. Strengthen the corporate risk function to be a leader of climate risk management. Provide risk teams with tools and training to assess, manage, and mitigate both physical and transition risks. Integrate climate resilience considerations into corporate strategy and decision-making processes, aligning with the organisation's net zero commitment.

Climate change is increasing the need for resilient infrastructure. Organisations must understand the physical and transition climate risks impacting their infrastructure, the effects on customers and what appropriate infrastructure availability looks like in a changing world. Asset owners have a responsibility to provide a service to customers, but also a legal responsibility to keep customers safe.

While not all assets can be protected from climate change impacts, by managing risks effectively, infrastructure owners can proactively engage customers to minimise the impacts of climate events. Asset owners must also manage customer expectations and communicate the impact of climate change on their infrastructure, improving reliability and resilience. Finally, by understanding risks, making balanced investments in modernisation and adaptation, and empowering risk management, asset owners and operators can enhance infrastructure resilience whilst contributing to a sustainable future.

How KPMG can help

Our multi-disciplinary team of enterprise risk professionals from KPMG's global network of member firms has extensive experience across all aspects of integrated risk and resilience. In the Middle East, our recent experience comprises operational resilience and third-party risk management engagements with some of the country's largest organisations.

Our integrated governance, risk and compliance services:

- Next generation risk and resilience strategy, operating models and tooling.
- Risk and resilience governance, organisation and culture.
- Resilience by design framework and implementation.
- Integrated scenario testing design and execution.
- Customer value proposition, communications and assurance.
- Remediation strategy and vulnerability management.
- TPRM optimisation, contract management, exit planning and testing.
- Climate risk assessment.
- Cyber and technology resilience.
- People, data and infrastructure resilience.
- Crisis and incident management and reporting.
- Strategic tooling solutions: requirements definition, implementation and embedding.
- Independent assessment and assurance reviews.

Contacts

Sudhir Arvind
Partner
Head of Enterprise Risk Services
KPMG Middle East
sarvind@kpmg.com

Tejas Mehta
Partner
Business and Technology Resilience Lead
KPMG Middle East
tmehta4@kpmg.com

Ashley Harris
Partner
Operational Resilience
KPMG in the UK
ashley.harris@kpmg.co.uk

Ali Abedi
Director
Business and Technology Resilience
KPMG Middle East
aabedi2@kpmg.com

Publication name: Operational resilience
Publication number: 5724
Publication date: November 2025