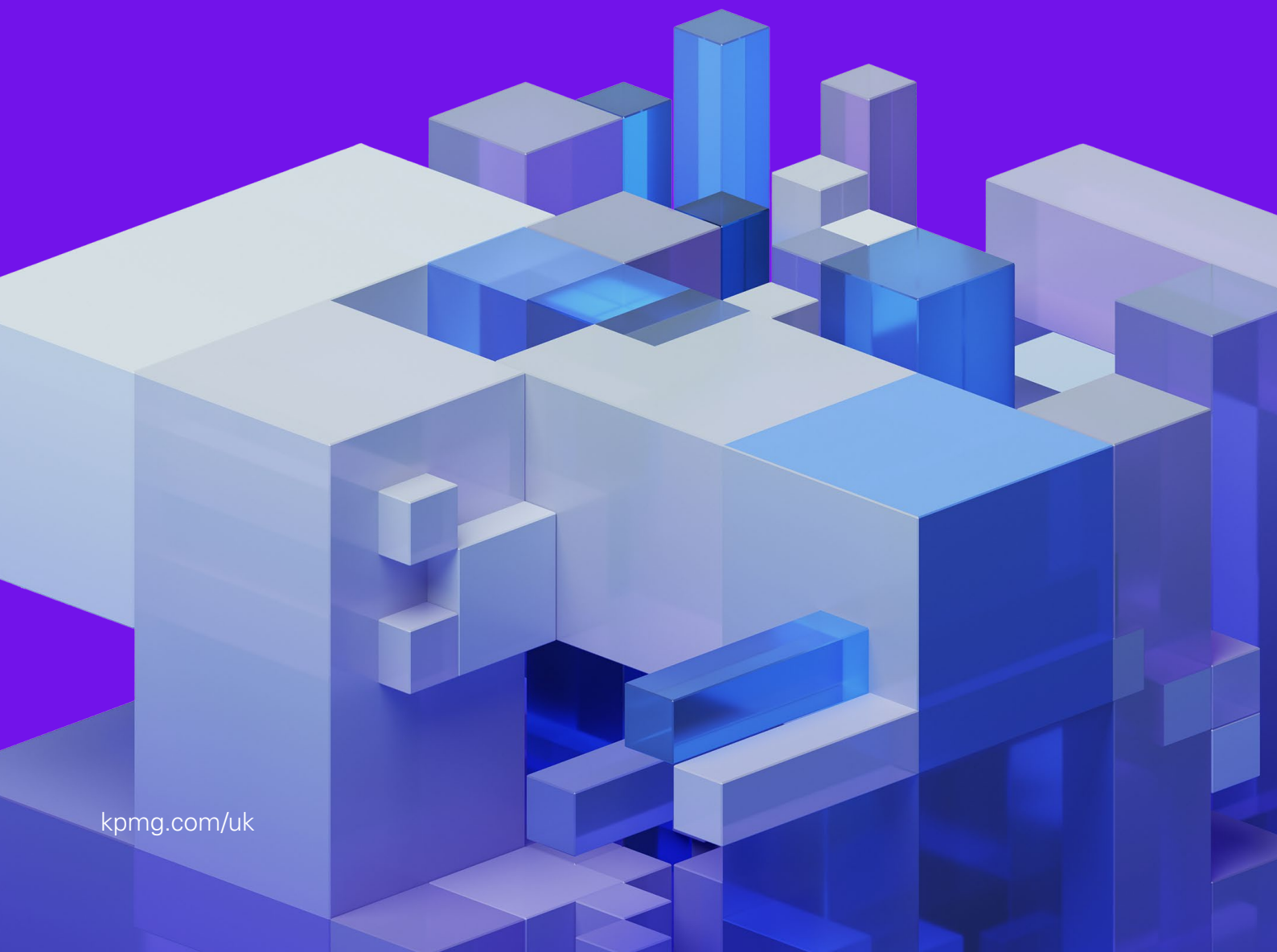
KPMG

Building a Resilient Ecosystem

Collaborating For Success



kpmg.com/uk

Contents

Operational Resilience: A Competitive Advantage

In recent times, no other word in the dictionary has had a bigger evolution in its connotation than the word "Normal". What was considered an exceptional occurrence is now the (new!) normal.

Firms have long been operating in an environment of interconnected and overlapping crisis. All signs indicate that Polycrisis is the new normal. 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. Are you in?

3 actionable approaches to build and operationalise a sustainable Operational Resilience capability:

1. Accountability & 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 & 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 & C-suite 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 & 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.

Simran Singh
Director
Operational Resilience
KPMG in the UK

Operational Resilience: Beyond Internal Recovery to Mitigating External Harm

Financial services firms have long engaged in various forms of testing to ensure business continuity (BC). Whilst BC, IT Disaster Recovery (ITDR), Incident, 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.

Steven Horgan
Manager
Operational Resilience
KPMG in the UK

Tom Henshaw
EMEA Head of Platform
Go-To-Market
Fusion Risk Management

The Gap: 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 / RTO / RPO, 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 for Mitigating External Harm

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 extrnal end users. This also involves assessing the effectiveness of communication strategies and any third-party support mechanisms.

From Desktop to Live Testing: 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 Important Business Services.

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.**

How Fusion Can Help: Informed Scenario Selection and Enhanced Testing

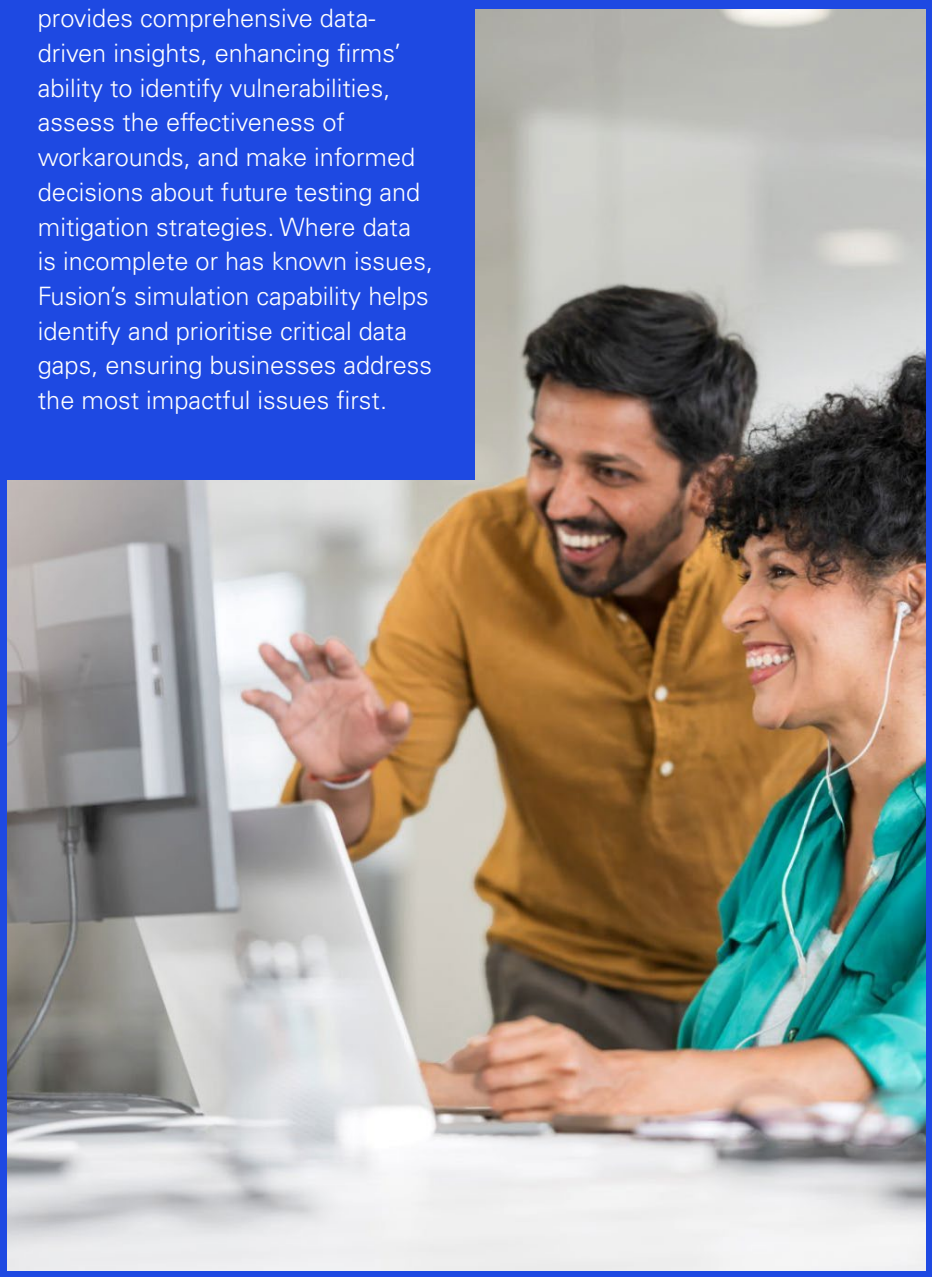
Live testing presents several challenges. It can be risky, as it potentially involves disrupting business operations as it requires the diversion of resources and attention away from BAU activities. It can also be costly, requiring significant resources and time. Given these challenges, it is crucial to ensure that each test provides maximum value. Fusion, a software solution designed specifically for Operational Resilience, can help firms optimise live testing by:

- **Minimising Disruption**: Fusion's advanced simulation capabilities allow for realistic testing without impacting live operations to enable firms to select appropriate scenarios for live testing. This reduces the risk of disrupting BAU and ensures a smoother testing process.
- **Streamlining Resource Allocation**: Fusion's automated features streamline the testing process, reducing the need for manual effort and freeing up valuable resources. This helps optimise resource allocation and minimise the cost of live testing.

Fusion's Scenario Testing capabilities also deliver other significant benefits, including:

- **Scenario Prioritisation**: Businesses are exposed to an increasingly wide variety of operational threats, ranging from evermore frequent natural disasters to data breaches and cyber-attacks. Using its Scenario Testing capability, which uses data science modelling and AI to analyse data and identify the most likely and impactful scenarios, Fusion can pinpoint the scenarios that have the greatest impact on IBS. This allows firms to prioritise live testing scenarios that will provide the most valuable insights, ensure the effectiveness of their mitigation strategies and enhance operational efficiency during the testing process.
- **Targeted Testing**: Fusion empowers firms to understand potential areas of concern, enabling targeted live testing of specific aspects of the workaround process or IBS functionality. The tool's Scenario Testing capabilities automatically run thousands of variations of a scenario against the value chain of an IBS or any assets within it, providing insight into the likelihood of asset recoverability and impact tolerance breach. This data allows firms to conduct more focused live testing, reducing the scope of disruption and minimising impact on BAU.
- **Data-Driven Insights**: Fusion provides comprehensive data-driven insights, enhancing firms' ability to identify vulnerabilities, assess the effectiveness of workarounds, and make informed decisions about future testing and mitigation strategies. Where data is incomplete or has known issues, Fusion's simulation capability helps identify and prioritise critical data gaps, ensuring businesses address the most impactful issues first.

Operational Resilience requires firms to shift from an internal focus to a more integrated approach that encompasses both internal recoverability and external harm mitigation. By embracing live testing and leveraging tools like Fusion, firms can enhance their testing programmes and ensure that they are well-equipped to continuously mature their Operational Resilience capabilities, protect their customers and the industry from the impact of disruptions, and navigate the evolving regulatory landscape.



Unlock the Power of Integrated Third Party Risk Management Data, Metrics and Reporting

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-Party 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.

Jon Dowie
Partner
Financial Services Technology Risk
KPMG in the UK

Rohit Nag
Director
TPRM Lead
KPMG in the UK

Emil Kalimullin
Director
T&D Modelling
KPMG in the UK

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.

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.

Key Focus Areas

Many organisations face challenges in effectively managing their Third-Party Risk Management (TPRM) data and reporting. Companies are seeking to overcome these hurdles by focusing on two key areas:

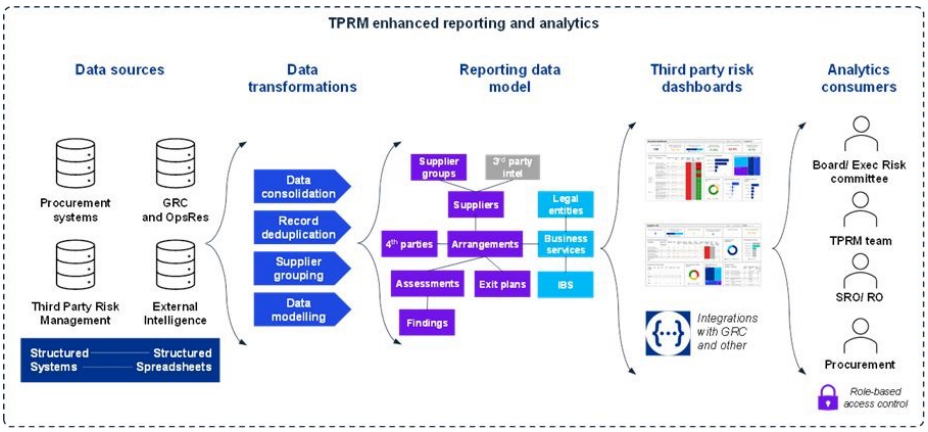
- **Integration of TPRM Data Sources**: By combining data from various sources — procurement systems, GRC platforms, risk assessment tools, and even spreadsheets — organisations can create a comprehensive view of their third-party risk landscape. This integration enables more accurate insights and better visibility into the overall risk profile.
- **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:

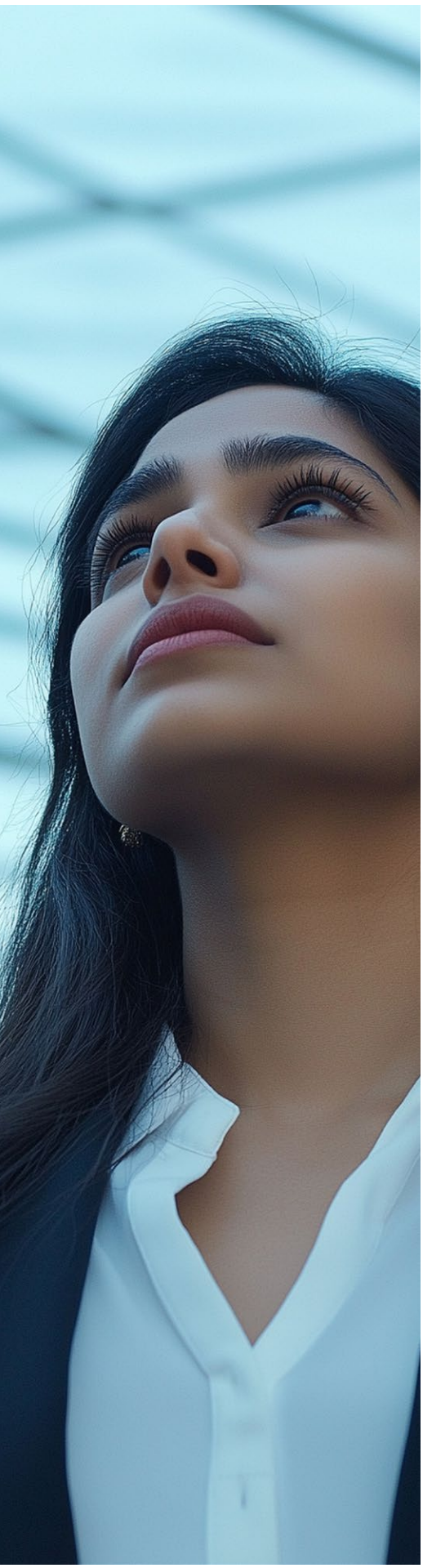


Actions to Take Now

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.



The Importance of Being Resilient by Design

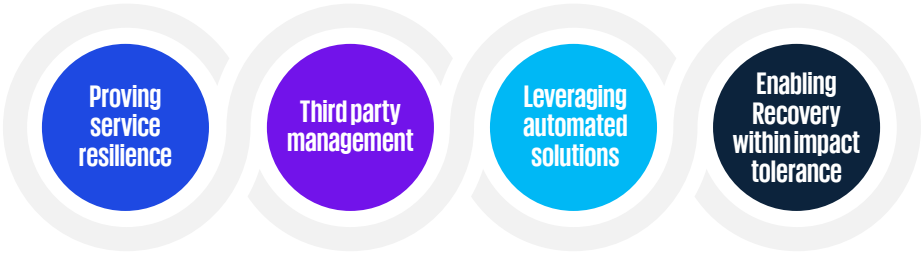
Resilience by Design is a new methodology that can help your organisation manage resilience gaps in the face of change and defend against emerging threats. In today's world, Operational Resilience is more critical than ever, with cyber-attacks, pandemics, and extreme weather events adding to ever-increasing challenges.

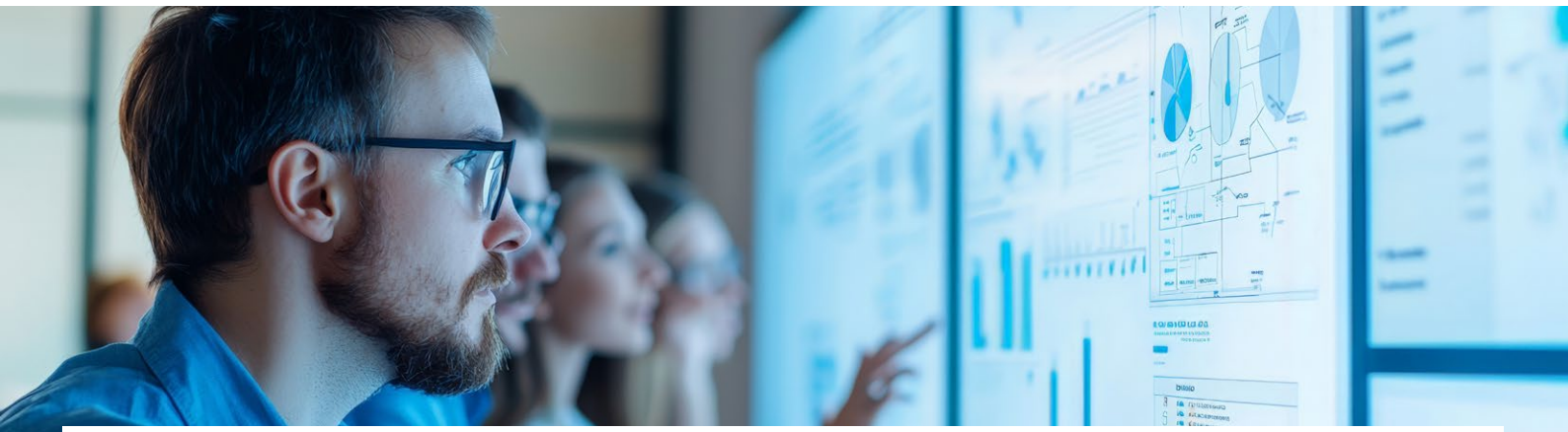
By adopting a principles-led, risk-based approach to managing change to Important Business Services, organisations can ensure that they continue to be well-prepared to weather any storm. Resilience by Design is a component part of an organisation's approach and complements the operating model, tooling,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

So, 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 Important Business Service 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.



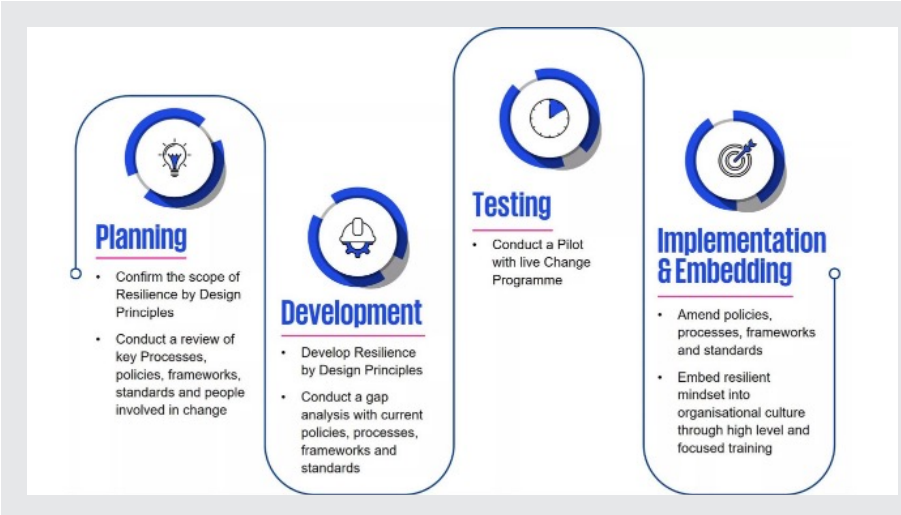


What do I need to think about when implementing Resilience by Design?

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 Important Business Services 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.

Steven Horgan
Manager
Operational Resilience
KPMG in the UK



It's not just a process, it's a change in 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 Important Business Services 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?

Navigating Complexity: How Fusion & KPMG Deliver Market-Leading Operational Resilience for Firms

In today's rapidly evolving business landscape, Operational Resilience has become a key focus for organisations across all sectors. Firms face an array of challenges: cyber threats, market volatility, regulatory shifts, and natural disasters, all while needing to maintain service levels to their customers.

This is where tooling solutions, like Fusion, can support. As a leading Operational Resilience software solution, Fusion empowers firms to anticipate, prepare for, and recover from disruptions, ensuring business continuity and safeguarding stakeholder interests. KPMG's alliance with Fusion combines Fusion's technological capabilities with KPMG's Operational Resilience expertise to provide industry-leading Operational Resilience solutions to firms.

What is Fusion and how can it help firms?

Fusion is a comprehensive software solution that empowers organisations to build resilience, manage risk effectively, and navigate crises with confidence.

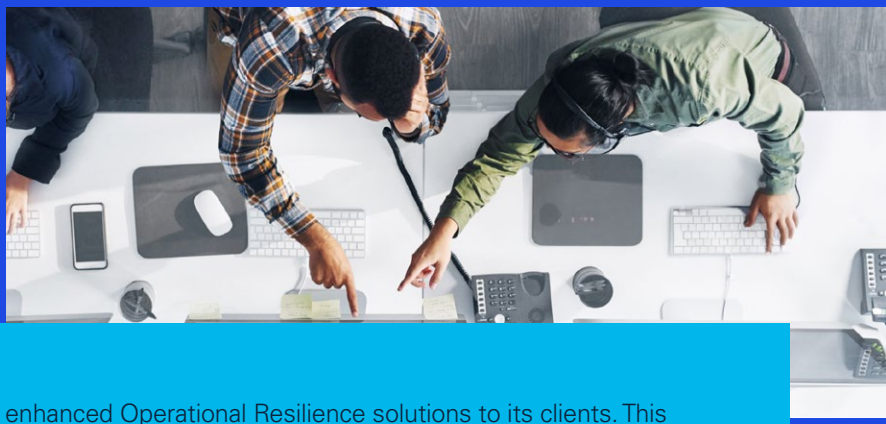
It provides a centralised platform for Operational Resilience, risk, and crisis management, enabling organisations to operate more effectively, reduce costs, mitigate risks, ensure compliance, and seamlessly integrate functional capabilities with enabling technologies. Fusion can empower your organisation to:

- **Proactively Prevent Outages**: Understand upstream and downstream dependencies, vendor vulnerabilities, and potential risks, like those experienced by CrowdStrike.
- **Streamlined Business Continuity**: Fusion's tailored software solution optimises business continuity plans for firms. By automating anticipation, prevention, preparation, testing, and response, all underpinned by data-driven insights, Fusion ensures critical operations continue seamlessly during disruptions.
- **Enhanced Collaboration and Integration**: Leveraging Salesforce's flexibility, Fusion seamlessly integrates a firm's architecture, fostering collaboration and promoting an end-to-end resilience approach.
- **Data-Driven Decision Making**: Fusion automates data gathering, empowering business functions with the insights and tools needed for informed decision-making. This automation reduces manual effort, freeing up employees' time to focus on high-value activities.
- **Compliance and Operational Excellence**: Fusion supports compliance with regulatory requirements and enhances operational effectiveness by addressing pain points associated with outdated resilience efforts. Combined with KPMG's expertise, Fusion helps companies exceed industry standards and optimise their operational processes.

Fusion's Solutions

Fusion is a powerful platform with a comprehensive and flexible suite of capabilities that can empower and accelerate any risk and resilience team within your organisation. Some examples of how Fusion's innovation can support your approach to Operational Resilience include:

- **Harnessing the Power of Fusion Expertise with AI**: Fusion Intelligence is a generative AI-powered expert analyst. Leverage years of resilience and continuity experience, best practice guidelines, and expertise built-in to your solution, to help your team to strengthen your resilience posture. Use Fusion's AI Agent to take action on your behalf and mature your resilience data, and ingest unstructured, static documents into structured, actionable resilience data automatically using Fusion.
- **Leveraging AI for Scenario Testing**: Fusion's Scenario Testing capability is the latest revolutionary approach for modelling scenarios against your business and forecasting impact before it materialises. With Scenario Testing, your organisation can seamlessly generate a range of potential events, test critical scenarios, understand cascading impacts, and gain a comprehensive understanding of your vulnerabilities, giving you the confidence to make the right decisions under pressure as well as prioritise desktop and live scenario testing activities.
- **Integrating with Products such as AlertMedia**: Through this particular integration, you can benefit from an integrated resilience hub that delivers bi-directional data and event syncing, real-time threat intelligence, faster two-way mass notification capabilities, and increased collaboration that ensures more informed and speedier recovery.



Fusion and KPMG's relationship

KPMG has formed an alliance with Fusion to deliver enhanced Operational Resilience solutions to its clients. This collaboration leverages KPMG's extensive industry knowledge and implementation experience of Operational Resilience and Fusion's innovative technology to provide tailored solutions that meet the unique needs of each firm.

KPMG has worked closely with regulators, including the PRA and FCA, to develop a framework that has been extensively deployed across the UK Financial Services sector. Its team of industry experts can advise and support clients across the end-to-end resilience lifecycle, from design through to implementation.

KPMG's Operational Resilience framework is based upon best practice and lessons learned to support firms in avoiding common implementation challenges. KPMG's broader expertise in risk management, regulatory compliance, and business transformation complements Fusion's capabilities, ensuring that clients receive a comprehensive suite of services as they look to build and embed a resilient lifecycle into business as usual.

Operational Resilience is no longer a "nice-to-have", it's a necessity. By embracing a proactive approach and leveraging solutions like Fusion, firms can build a robust foundation for resilience, ensuring business continuity and customer satisfaction in the face of any disruption.

Steven Horgan
Manager
Operational Resilience
KPMG in the UK

Tom Henshaw
EMEA Head of Platform
Go-To-Market
Fusion Risk Management

KPMG FUSION RISK MANAGEMENT

Resilience to Climate Change: Impacts on Infrastructure Availability and Users

The Impact of Climate Change on Our Infrastructure

In recent years, the UK has experienced record-high temperatures and the wettest winter in 130 years. 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 UK's commitment 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 winds 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 2015, Storm Desmond caused unprecedented flooding in the UK, highlighting the vulnerability of infrastructure to climate change. Despite investments in flood defences, the economic impacts of the flooding exceeded £400-500 million. Infrastructure failures included damaged bridges, disrupted traffic lights, and power outages, affecting critical services.

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.

In 2020, an inadequately managed drainage system in Stonhaven was overwhelmed by heavy rain, triggering the worst British railway accident in 18 years. Consequently, Network Rail received a £6.7m fine and have pleaded guilty to maintenance and inspection failures which led to three deaths.

This incident underscores the human, economic and legal responsibilities of asset owners for the services they provide.

Network Rail has committed to spending £2.8bn to help it adapt to the impacts of extreme weather and climate change. Other organisations must prioritise infrastructure resilience to mitigate such crises, protecting lives and safeguarding business continuity.

The Impact on Organisations

The repercussions of infrastructure systems failure due to climate events such as Storm Desmond are profound for organisations. The overall standing of the organisation is weakened by monetary penalties, impaired market perception and investor/public confidence. The Stonehaven rail crash exemplifies the lasting effects of reputational damage resulting from inadequate climate risk management.

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.

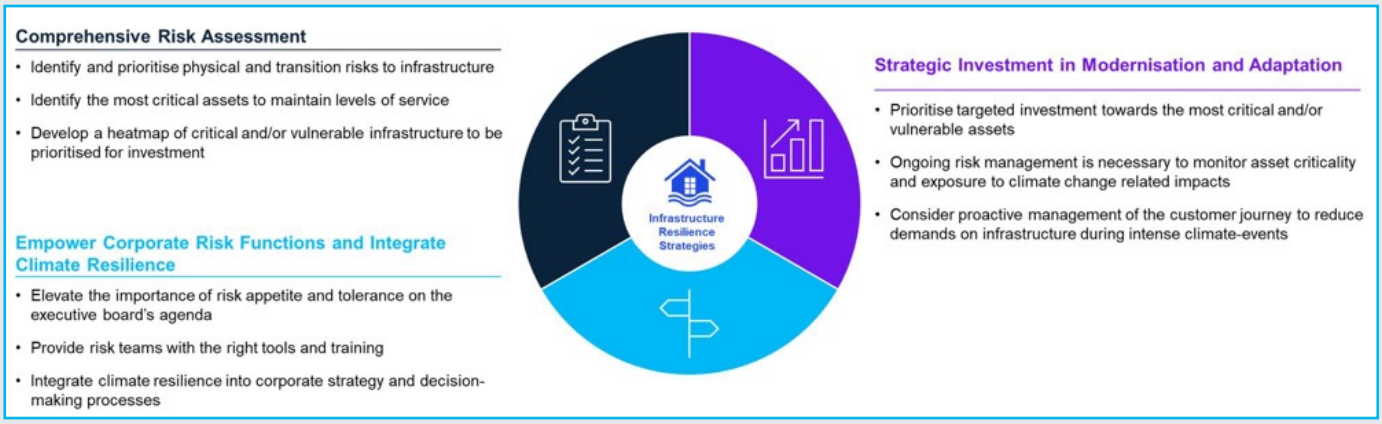
A path forward

Addressing climate change demands a proactive and strategic approach focused on understanding physical and transition risks. The UK Climate Change Committee emphasises 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 indiviudally or together to enhance your risk capabilities and ability to predict and respond to the impacts of climate change.



Comprehensive Risk Assessment

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.

Strategic Investment in Modernisation and Adaptation

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.

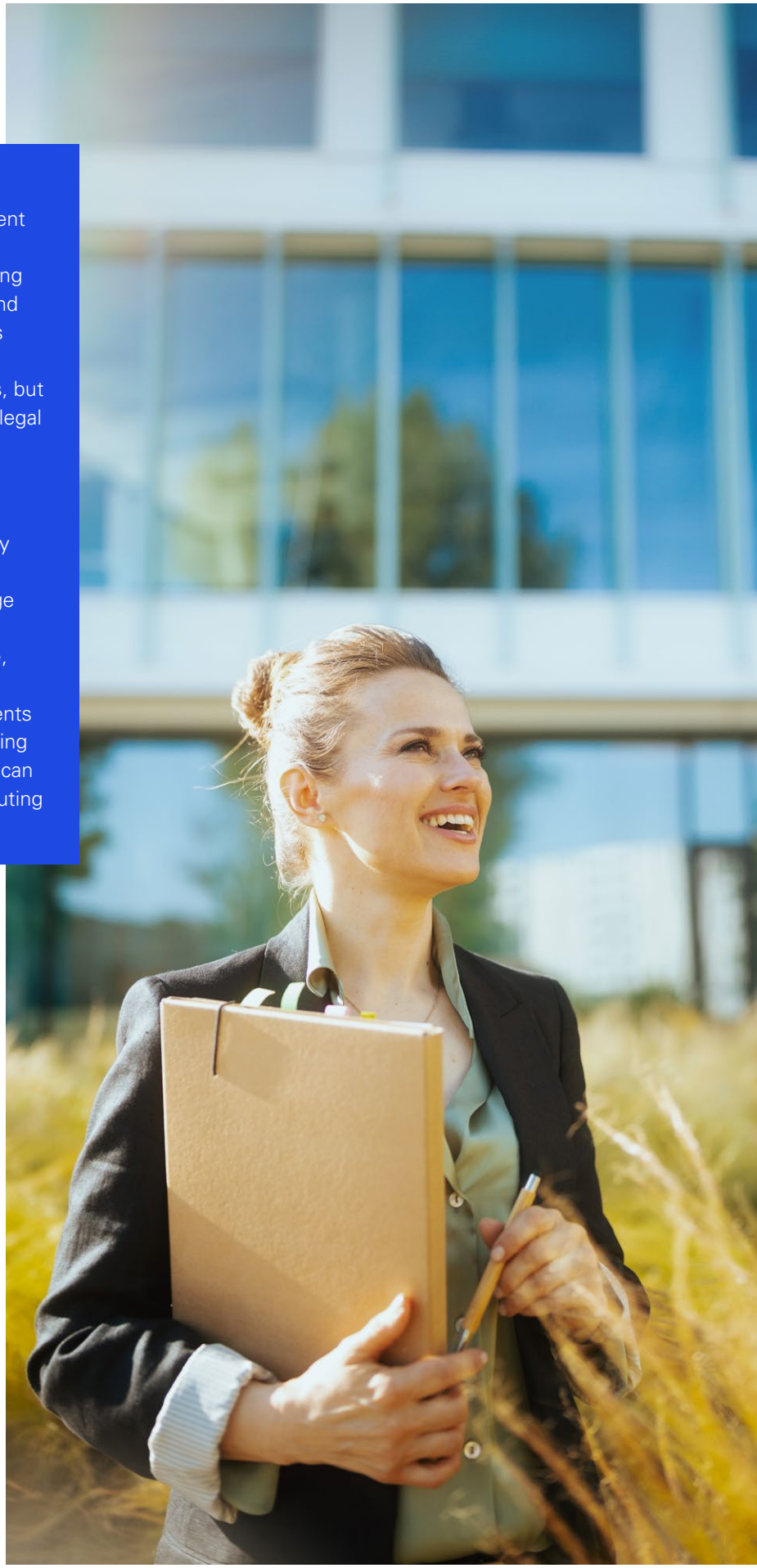
Empower Corporate Risk Functions and Integrate Climate Resilience

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.

Conclusion

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 as the Stonehaven example highlighted, 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.



Sebastian Wooff
Assistant Manager
Customer, Operations & Infrastructure
KPMG in the UK

Ioanna Papanikolaou
Associate Director
Customer, Operations & Infrastructure
KPMG in the UK

Alan Taggart
Partner
Customer, Operations & Infrastructure
KPMG in the UK

Six Operational Resilience Lessons Learnt from the CrowdStrike Outage

The global technology outage caused by a software bug in CrowdStrike's quality control system highlights the critical importance of Operational Resilience and Third Party Risk Management.

We have seen a broad impact across all sectors, with the most pronounced effects being felt outside of financial services firms due to the financial regulatory agenda. However, it is important to note that the financial services industry has also been affected, and the following lessons learnt should be considered in the context of all sectors. This incident underscores the need for firms to carefully vet and monitor their third-party vendors, especially those providing critical services to Important Business Services. Here are some of our key takeaways:

Ashley Harris
Partner
Operational Resilience Lead
KPMG in the UK

Granularity of supply chain mapping

Many firms failed to map CrowdStrike either as a critical third-party or a fourth party service to their Important Business Services, despite its crucial role in internal technology and infrastructure. This highlights the need for more comprehensive and granular mapping of third-party dependencies into the fourth and nth parties who support critical services. Firms should move beyond simply identifying third-party vendors to understanding the specific services they provide and how those services impact their critical business functions. This detailed mapping will enable firms to better assess the potential impact of disruptions to these services and develop appropriate mitigation strategies to reduce the likelihood of intolerable harm being caused to vulnerable customers.

Black swan events are plausible

The outage demonstrates the plausibility of "Black swan" events that can disrupt entire business operations. Firms need to re-evaluate their scenario planning and consider the potential impact of such events on their Important Business Services. Traditional scenario planning often focuses on predictable risks, but firms must also consider the possibility of low-probability, high-impact events like the CrowdStrike outage. By incorporating these "black swan" scenarios into their planning, firms can develop more robust contingency plans and improve their overall resilience.

The need to follow an IBS-centric recovery approach

We have seen a number of post incident reports where firms have detailed their responses to recovering their essential services following the CrowdStrike outage. However, there appears to be a lack of an Important Business Service-centric approach to recovery whereby firms are viewing incidents through a prioritised lens of impacted services. Firms should consider establishing service recovery blocks, as well as well-defined and tested playbooks, which provide decision-makers with options and timeframes to enable efficient and effective decision-making through the lens of the firm's most critical services.

The need to define 'resilience by design' principles

The incident underscores the importance of "resilience by design" principles. Firms should implement robust frameworks to ensure that changes to critical third-party services are thoroughly tested and meet pre-defined resilience criteria before deployment. This includes establishing clear testing protocols, conducting thorough impact assessments, and developing rollback plans in case of unexpected issues. By adopting a "resilience by design" approach, firms could minimise the likelihood of disruptions caused by internal and third-party changes and ensure the continued availability of Important Business Services.

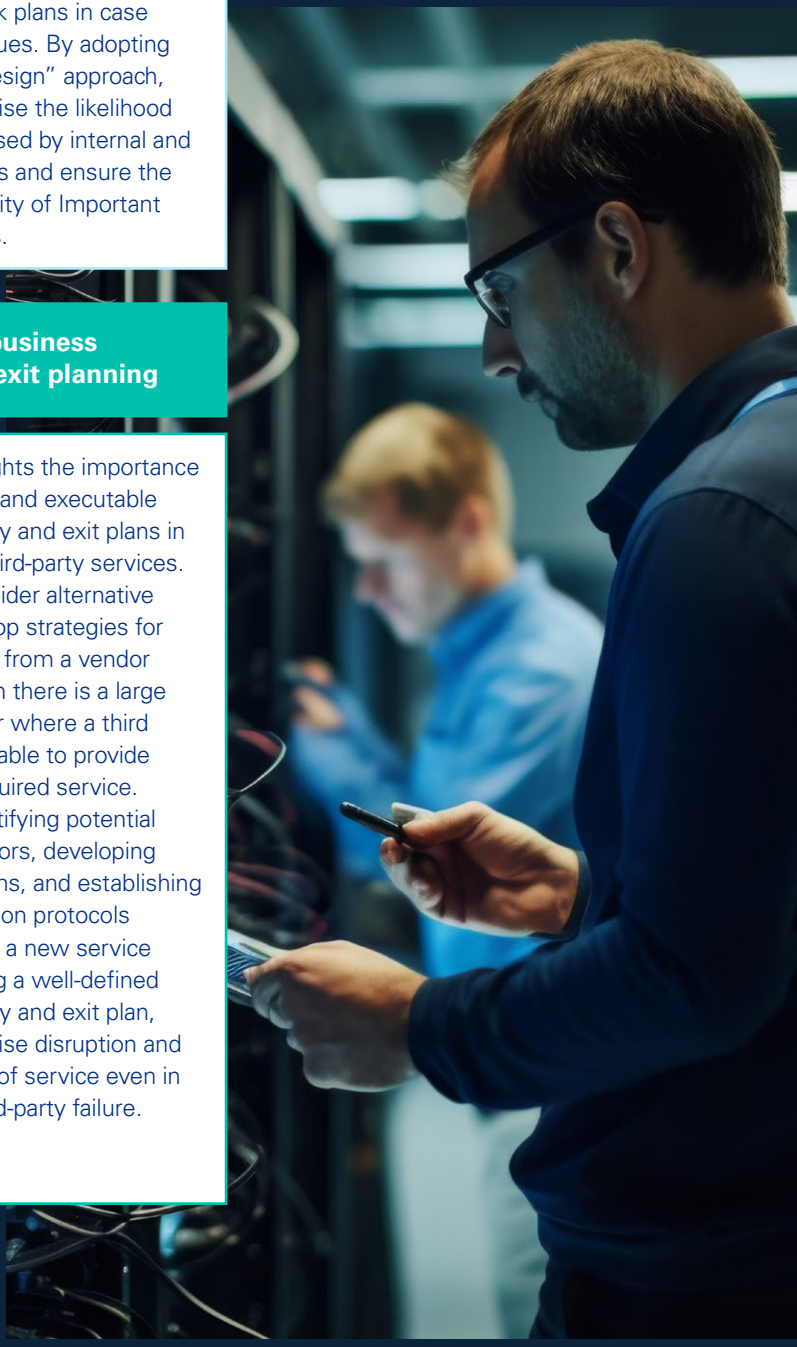
Importance of third-party criticality assessment and oversight

Firms must identify their critical third party service providers and hold them accountable for resilience and contractual requirements. This includes requesting evidence of adequate internal testing, control effectiveness, and adherence to contractual obligations. Firms should establish clear communication channels and incident management processes with their third-party vendors and regularly monitor their performance to ensure that they are meeting the agreed-upon standards. By actively overseeing their third-party relationships, firms could mitigate the risk of disruptions and ensure that their Important Business Services remain resilient.

Importance of business continuity and exit planning

The outage highlights the importance of having credible and executable business continuity and exit plans in place for critical third-party services. Firms should consider alternative options and develop strategies for transitioning away from a vendor if necessary, when there is a large disruption event or where a third party is no longer able to provide the necessary required service. This includes identifying potential replacement vendors, developing data migration plans, and establishing clear communication protocols for transitioning to a new service provider. By having a well-defined business continuity and exit plan, firms could minimise disruption and ensure continuity of service even in the event of a third-party failure.

The CrowdStrike outage serves as a valuable lesson for firms to strengthen their Operational Resilience and Third Party Risk Management practices. By implementing the recommendations outlined in this article, firms can mitigate the potential impact of similar incidents and ensure the continued availability of Important Business Services.



A Rapid Response to Regulatory Change at a European G-SIB

European G-SIBs, like all other financial organisations, are under constant pressure to meet ever-evolving regulatory expectations. Therefore, when the Prudential Regulation Authority (PRA) published its Policy and Supervisory Statement on Outsourcing and Third Party Risk Management (SS2/21) in March 2021, a European G-SIB bank wanted to understand how its existing capability fared against the new expectations.

The bank wanted any gaps resolved before the 31 March 2022 deadline, in order to carefully manage risk exposure. Therefore, the bank reached out to KPMG for help to understand the requirements and to get on track to meet them, quickly.

We put together an experienced team of Third Party Risk Management (TPRM) practitioners to carry out a thorough current state assessment of the bank's TPRM capability, focusing in particular on its material third-party arrangements. Our experts used KPMG's pre-built TPRM Maturity Assessment Tool to quickly identify the key gaps in the TPRM processes against the new expectations. We supported this with our tried and tested reporting template and visualisation to clearly outline priority actions, before working closely with the firm to develop a comprehensive project plan to uplift its TPRM capability.

The next steps were implementing changes.

Our team worked closely with the firm's project team to create a new end-to-end TPRM framework for the firm's UK business. The framework not only aligns to the PRA's regulatory requirements, but also caters to the spirit of the bank's group policies and procedures. By using KPMG's pre-built and pre-defined Powered Risk – TPRM accelerators, we were able to uplift the European G-SIB's framework rapidly within a 4-month timeframe. Key improvements made included: updated UK norms/policies; end-to-end TPRM processes, roles and responsibilities; materiality and inherent risk assessment; enhanced due diligence procedures; enhanced ongoing risk assessment procedures; and exit planning and testing templates and procedures.

As a result, the European G-SIB was able to meet its new regulatory expectations on SS2/21, and has a fit for purpose new TPRM framework that it can integrate and operate alongside its global framework and processes.

"KPMG have added significant value since we started working together. They have assisted by creating a standardised and risk-proportionate approach to Third Party Risk Management, across the end-to-end lifecycle. Throughout our engagement, KPMG brought in a great deal of regulatory knowledge and insight and were able to propose practical solutions to drive the project quickly and efficiently."

Head of Transversal Services, European G-SIB

Jon Dowie
Partner
Financial Services
Technology Risk
KPMG in the UK

Rohit Nag
Director
TPRM Lead
KPMG in the UK

Critical Third Party Resilience Regulation

UK regulators finalise new rules, broadening Operational Resilience scope to Critical Third Parties to the UK FS sector.

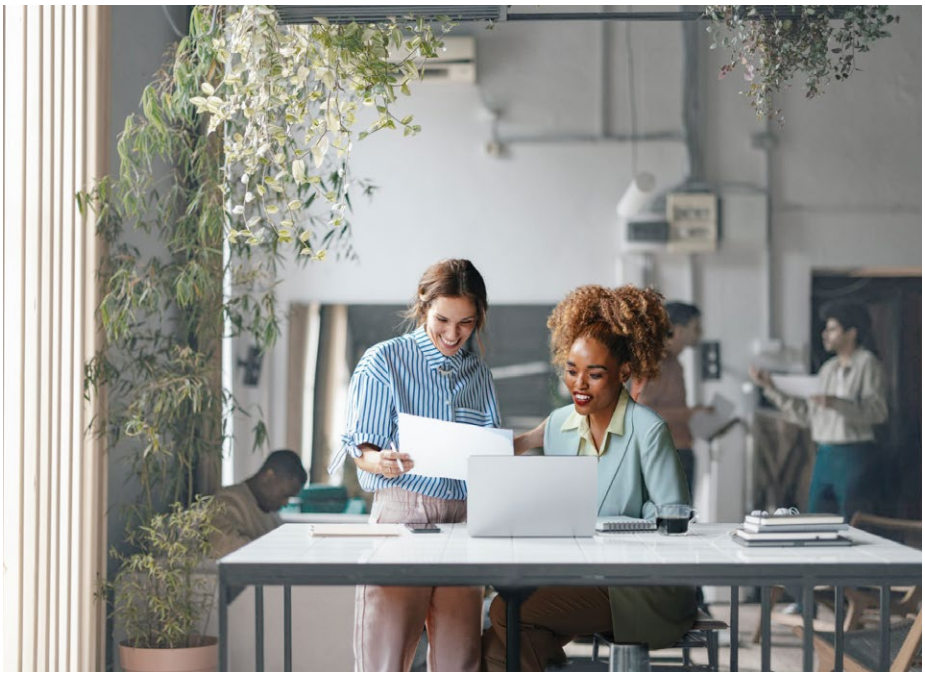
On the 12th November 2024, the Bank of England (Bank), Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) jointly issued a Supervisory Statement, Policy Statement and associated documents, setting out their final regulatory oversight regime for the Operational Resilience of Critical Third Parties (CTPs). The purpose of the new regulatory rules is to manage potential risks to the stability of, or confidence in, the UK financial system that may arise due to disruption to the services that a CTP provides to Financial Services (FS) firms and/or Financial Market Infrastructures (FMIs). The regulations define a systemic third party service as a 'service (wherever carried out) provided by a CTP to one or more firms, a failure in, or disruption to, the provision of which (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system.'

Georgia Hunter
Senior Manager
Operational Resilience
KPMG in the UK

Tom Henshaw
EMEA Head of Platform
Go-To-Market
Fusion Risk Management

Features of the New CTP Regulations

- **Designation**: While only HMT can designate a CTP, the regulators can recommend to HMT which third parties they consider meet the statutory test for designation. The list of the CTPs will be continually reviewed and updated to monitor for any third parties that may satisfy the statutory test in the future, as well as identify any suppliers where the CTP designation should be removed.
- **Granular Resource Mapping Approach**: A more granular set of mapping requirements has been outlined for CTPs. The critical processes and underlying assets across the 5 pillars (Technology, Data, Third Parties, People, Facilities) will need to be mapped, however consideration must also be given to energy suppliers and public communications operators. This will need to be completed within 12 months of designation. This is a shorter timeframe for completion and beyond the mapping requirements set out in the FS Operational Resilience regulations.
- **Enhanced Risk Processes**: CTPs will need to establish / enhance current risk processes so that there is a comprehensive and well-documented risk management system to monitor and address risks on an ongoing basis. Specific risk pillars include third party, cyber, technology, data, insider, facilities, energy supply and natural disasters.



- **Focus on Supply Chain Resilience**: CTPs will need to have a greater understanding of their extended supply chain (including key nth-party providers) and have the ability to identify and manage risks to the extended supply chain. Additionally, there must be appropriate measures to respond to a termination of any of its systemic services. This includes orderly termination and return of assets to the customer.
- **Incident Management Playbook Development and Testing**: CTPs will need to develop incident management playbooks for each of its system services which clearly articulates how the CTP will respond and recover from incidents within the maximum tolerance for disruption for each systemic service. This will need to be tested in collaborative incident management playbook exercises with a representative sample of the customer firms.
- **Increased External Incident Reporting**: Increased level of incident reporting will be required by CTPs. Firms in scope must be able to identify, monitor and report on material incidents impacting systemic services in an accurate, consistent and timely manner, including specific requirements for both interim and final incident reports.
- **Independent / Board Level Assessments**: An interim self-assessment must be developed by CTPs within the first 6 months of designation. Following that, ongoing annual assessments to be developed outlining the resilience activities by the CTP's Board and/or supervisory authorities. These assessments should also be shared with service recipients (ie. regulated firms).

What does this mean for the third parties supporting the FS industry?

- This policy is an attempt to introduce some element of alignment in resilience standards between regulated firms and their CTPs. CTPs will now need to meet resilience and risk management standards equivalent to the FS industry, and prepare for regulatory scrutiny.
- Given designation may change, there is likely to be a 'ripple' effect across the sectors in which third parties designated as critical operate (e.g. cloud services, data services etc). Other third parties may look to proactively implement and embed some of these requirements within their own organisation.
- There is a clear focus through this policy on introducing enhanced risk management standards more broadly across the CTP's organisation. This suggests that regulatory authorities have some fundamental concerns over the way non-regulated CTPs currently manage and monitor broader operational risk.
- A natural extension of these resilience standards across the broader supply chain is expected over time, thereby further enhancing the resilience of the extended supply chain.
- The level of detail and transparency of information shared between CTPs and regulated firms through the self-assessment will need to become clearer and what the long-term impact (if any) is for both service pricing and performance related pricing.

Tooling

The granular resource mapping requirements of PS16/24 – mapping services, critical processes and the underlying assets across Technology, Data, Third Parties, People, and Facilities – is a complex data mapping exercise that requires a detailed understanding of the many-to-many relationships that exist across an enterprise. Leveraging tooling to support this exercise ensures that mapping is delivered robustly and can be relied upon when it matters most. Tooling enables firms to accurately map the risks and controls for each asset to the processes and services that they support, highlighting where critical dependencies and vulnerabilities exist and which remedial measures are required. It provides a contextualised, business-informed view of those assets and the risks they pose to the firm, and enhances the ability to allocate resilience investment to the assets that need it most.

This business-informed understanding of risk applies across risk domains – third party, cyber, technology, data, insider, facilities, energy supply and natural disasters. By contextualising data from each of those risk domains using tooling, specialist teams can collaborate more effectively because they share common metrics and objectives – reducing risk and building resilience across the firms' most critical services and products. It articulates risk in terms that senior management comprehend and, armed with the correct tooling, enables leaders to make defendable, data-informed decisions that stand up to scrutiny when it matters most.

When an incident materialises, quick access to quality data is vital – and so is the ability to interrogate it, exploit it, and surface insights about the firm that will enable it to recover with minimal impact. The correct tooling enables firms to act dynamically during incidents as they unfold, to equip the right people with the data they need to make informed decisions, and to automate burdensome, time-consuming activity so practitioners can focus on strategic, forward-looking activity that will protect the firm, its customers and wider market.

By leveraging the power of software, resilience leaders can identify vulnerabilities proactively, mitigate emerging threats early, mitigate risk before it materialises, and stay ahead of incidents as they unfold. The correct tooling elevates the profile of the resilience function and puts it at the centre of organisational decision making. Tooling should provide a robust data model that acts as the nerve centre of the enterprise – informing firms where they may break, showing which vulnerabilities need prioritisation, and which remedial measures will build resilience where it matters most.

For more information please get in contact with Georgia Hunter (KPMG), or Tom Henshaw (Fusion).

UK Regulatory Consultation Papers on Updated Reporting Requirements for Operational Incidents and Third-Party Reporting

The UK financial services sector continues to face operational disruptions, impacting both consumers as well as the stability of the wider UK economy.

In an effort to continually improve the management of incidents and associated post-incident analysis, the Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) released consultation papers in December 2024 outlining proposed Operational Incident and Third-Party Reporting requirements for UK FS regulated firms.

Th consultation papers CP17/24 and CP24/28 aim to bolster existing resilience frameworks, ensuring consistent, sufficient, and timely reporting to minimise the impact of operational disruptions. The consultation papers propose new rules and expectations for two key areas.

1. Operational incidents reporting
2. Outsourcing and Third-Party Reporting

1. Reporting Operational Incidents

Incident Assessment

The FCA and PRA have set clear expectations for firms to provide sufficient and timely information about operational incidents that breach one or more thresholds. The regulators are proposing that:

- An operational incident will need to be reported to the FCA if a threshold is breached, namely if there is an actual or potential risk to: consumer harm, market integrity and safety & soundness.
- An operational incident report will need to be submitted to the PRA if an operational incident poses a risk to the stability of the UK financial sector, safety and soundness of the firm and the appropriate degree of policyholder protection (for insurers).

To determine whether an incident should be reported to the regulators, firms will need to assess the impact of an incident against the consumer, market and firm thresholds whilst considering factors such as direct and indirect impact on clients/consumers and the wider sector, the firm's ability to continue to provide adequate services, any impact on either the firm's or sector's reputation and the firm's ability to meet legal and regulatory obligations.

Reporting Requirements

The papers propose a phased approach to incident reporting, requiring firms to submit initial, intermediate and final reports.

1. Initial Report: If a threshold has been met, firms would be required to submit an initial report as soon as practical but no later than 24 hours of determining an incident has met a threshold.
2. Intermediate Reports: Firms must submit intermediate reports when there are significant changes in the incident's status or impact, providing updates on the incident's management and any actions taken.
3. Final Report: After the incident is resolved, firms must submit a final report within 30 working days, providing a full assessment of the incident's impact, root cause, lessons learned, and any additional steps taken.

The proposed reporting templates included in the Consultation Papers are extremely detailed, and will require firms to gather and share a new level information within the initial hours of an incident. Many firms currently have limited capability to provide the information being proposed and some believe that producing such detailed reports during an incident could distract from actually resolving the incident and recovering services to end users.

2. Outsourcing and Third-Party Reporting

The FCA and PRA are proposing to:

- Expand the scope of existing outsourcing notifications, covering both material outsourcing and material non-outsourcing arrangements (collectively referred to as 'material third-party arrangements') for in-scope firms.
- Provide a template for firms to submit notifications of changes to these arrangements or new ones.
- Set requirements for firms to maintain and submit a register of these arrangements to them, ensuring this is up to date annually.

Third-party Arrangements

The FCA proposes a new definition of "third-party arrangement" to encompass both outsourcing and non-outsourcing arrangements, focusing on those that are "material" to the firm's operations.

The PRA proposes to expand its data collection on third-party arrangements to include all material arrangements, not just outsourcing. This is because firms are increasingly reliant on a wider range of third-party services, and managing the risks associated with these arrangements is crucial for Operational Resilience.

Notifications

Both the PRA and FCA are proposing changes to their notification requirements for material third-party arrangements, aiming to expand the scope of notifications and standardise reporting including notifications to include all material third-party arrangements, including both outsourcing and non-outsourcing arrangements. The PRA also proposed a standardised template for notifications to provide clear expectations and reduce reporting burden.

Register of 3rd Party Arrangements

The FCA and PRA set expectations for firms to maintain and submit to the regulator a structured register of their third-party arrangements. Firms must submit their registers annually, containing information including regulated firm details, third-party details, including intra-group arrangements, the types of services performed by third parties and supply chain information.

This information would allow the regulators to improve its oversight of firms' reliance on third parties by assessing compliance, understanding risks, collecting insights, and monitoring the sector's reliance to identify potential Critical Third Parties (CTPs). It is expected that most firms will still be required to perform a considerable amount of work to collate their third-party risk data to the level of detail being proposed. Firms also have concerns around the current quality and completeness of the data required as inputs into the Register.

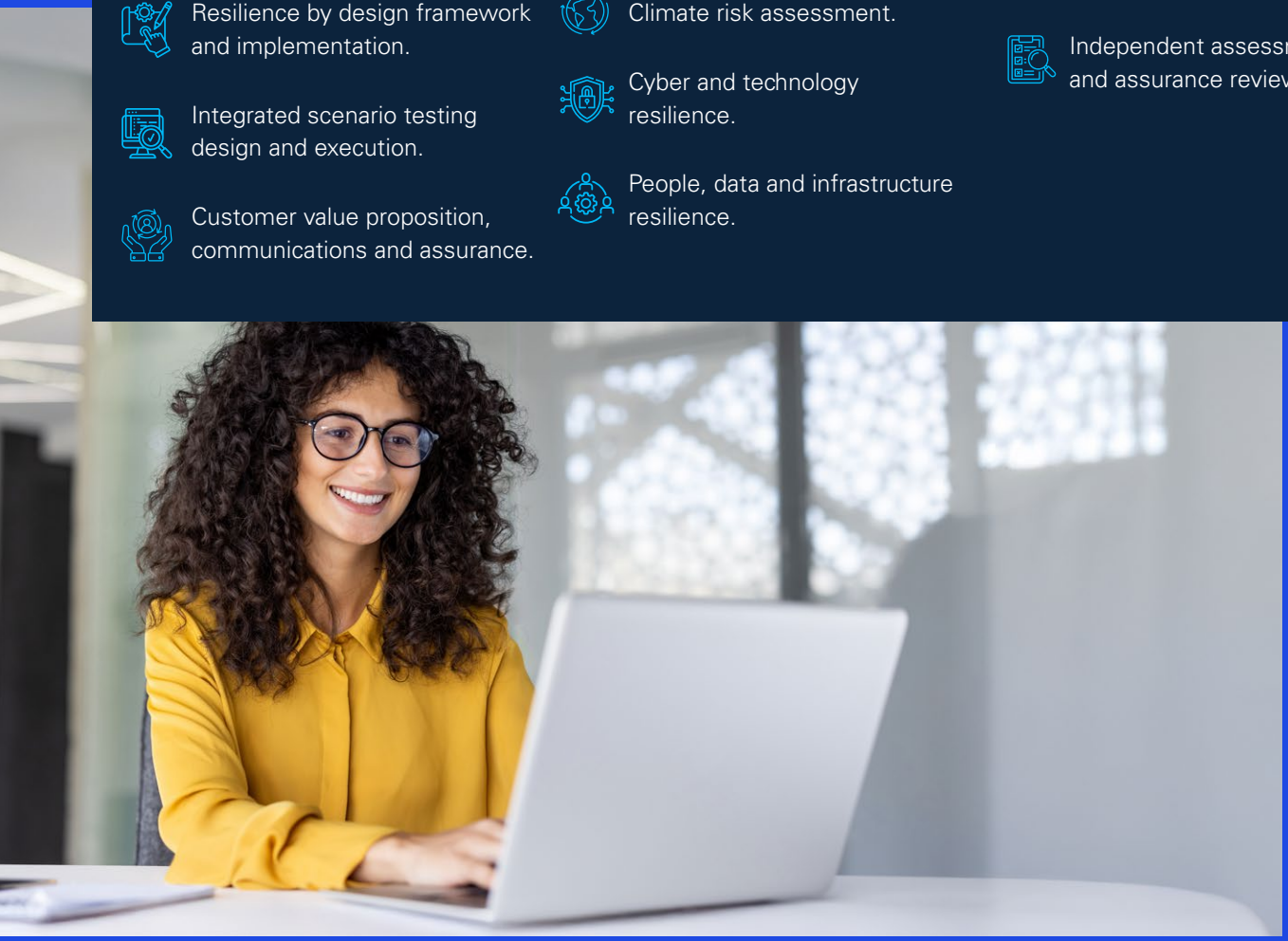
Georgia Hunter
Senior Manager
Operational Resilience
KPMG in the UK

How KPMG Can Help

Our multi-disciplinary team of SMEs from KPMG's global network of member firms has extensive experience across all aspects of integrated risk and resilience. Our recent UK experience comprises over 300 Operational Resilience and Third Party Risk Management engagements.

Our Integrated Risk & Resilience Services:

- Next generation risk & resilience strategy, operating models and tooling.
- Risk & 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 & incident management and reporting.
- Strategic tooling solutions: requirements definition, implementation and embedding.
- Independent assessment and assurance reviews.



Get in Touch

We have a multi-disciplinary team that can support your wide-ranging Operational Resilience and Third Party Risk Management requirements. Please reach out to the contacts below for more information.

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

Andrew Husband
Partner
KPMG Fusion Alliance Lead
KPMG in the UK
andrew.husband@kpmg.co.uk

Rohit Nag
Director
TPRM Lead
KPMG in the UK
rohit.nag@kpmg.co.uk

Simran Singh
Director
Operational Resilience
KPMG in the UK
simran.singh2@kpmg.co.uk

Georgia Hunter
Senior Manager
Operational Resilience
KPMG in the UK
georgia.hunter2@kpmg.co.uk

kpmg.com/uk

Designed by CREATE | CRT159928