KPMG

Operational Resilience

UK Regulatory Consultation Papers
KPMG perspectives

January 2020

kpmg.com/uk

Contents

1. Context & introduction

> "As a consequence, the policy proposals we are bringing forward for consultation, we believe, go with the grain of thinking in the industry. While these proposals are tailored to the individual policy frameworks and supervisory approach of each respective authority, they share a common overarching approach to Operational Resilience. We strongly encourage firms to take ownership of their own Operational Resilience and to prioritise based on the impacts to the public interest, as represented by the authorities' objectives."
>
> **Building Operational Resilience: Impact tolerances for important business services**

Since the BoE / PRA / FCA Discussion Paper on Operational Resilience was issued in July 2018, KPMG has had the privilege of working with many of our clients in developing strategy and supporting execution, and following the release of the regulatory Consultation Papers, having analysed the content, we are issuing this report to provide a summary, setting out:

1. What is new in the papers;
2. KPMG's point of view; and
3. What it means for firms in scope.

This report sets out insights from several of our Operational Resilience subject-matter experts, addressing the content of the following papers:

- CP19/32: Building Operational Resilience: impact tolerances for important business services and feedback to DP18/04 – issued by FCA;
- CP29/19: Operational resilience: Impact tolerances for important business services – issued by BoE/PRA;
- CP30/19: Outsourcing and third party risk management – issued by BoE/PRA;
- CP: Operational Resilience: Central Securities Depositories – issued by BoE/PRA;
- CP: Operational Resilience: Recognised Payment System Operators and Specified Service Providers – issued by BoE/PRA; and
- CP: Operational Resilience: Central Counterparties – issued by BoE/PRA.

In analysing the papers, it is important to understand the context in which the industry now operates, particularly the factors listed below:

- The intensity of technology innovation;
- Extended supply chains;
- A relentless focus on cost;
- 24/7 customer expectations;
- The changing nature of threats;
- The immediate visibility of incidents; and
- The complex political environment in which we all operate.

> "A key priority for the Bank of England (BoE), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) is to put in place a stronger regulatory framework to promote Operational Resilience of firms and financial market infrastructures (FMIs)."
>
> **Building Operational Resilience: Impact tolerances for important business services**

In light of these, and the constantly accelerating rate of change, it is hardly surprising that many of the business services that our consumers and markets are most dependent upon now require urgent attention. In many cases, the delivery solutions for these services were designed and implemented in an altogether different era.

The good news is that throughout the discussion period we have seen the development of a positive and fruitful collaboration between UK regulators and the industry and we now have a constructive and realistic set of proposals for Operational Resilience outlined in these Consultation Papers.

It is now clear that firms will be required to put in place robust management frameworks to prioritise and allocate investment to deliver resilience across important business services. From this point we are currently expecting final policy in late 2020, all the rules would then take effect a year after publication, and firms will then have longer (up to three years) to be able to show they are able to remain within impact tolerance for their important business services.

2. Key regulatory themes

It is worth summarising the key themes before looking in more detail at some of the main developments in the regulators' approach to this subject.

- Operational resilience must be driven from the Board with clear accountability for differentiated investment decisions that properly consider resilience.
- Resilience should be prioritised for Important Business Services, those services that have the greatest potential to cause harm to consumers, the financial system and the firm itself.
- The resources that a firm deploys to deliver those most important services must be mapped across Technology, Data, People, Facilities, Suppliers and now key Dependent Processes.
- The maximum tolerable level of disruption to an important business service must be defined as an impact tolerance, and metrics must be identified to monitor and measure the firm's ability to remain within the tolerance.
- Firms should identify severe but plausible scenarios to test the ability to respond and recover within those tolerances.
- Robust internal and external communications plans must be in place to manage the impact during any service disruption – with an emphasis on ensuring the timeliness and accuracy of the information provided.
- Firms must demonstrate that they have taken decisive and effective actions to improve resilience and have embedded a recovery centric mind-set within the organisation's culture.

In the following sections, we explore some of the main areas where we have identified changes, additions or clarifications that have been made since the Discussion Paper came out.

> "Operational resilience is not about protecting the reputation of your firms or the reputation of the industry as a whole. It is about preventing operational incidents from impacting consumers, financial markets and UK financial system. We will not accept operational failures that – but for a lack of sufficient contingency planning – see consumers stuck on the phone for hours trying to speak to their bank, unable to complete a house sale or purchase or facing uncertainty over whether they will be able to pay their rent on time because they cannot transfer their money."
>
> **Megan Butler, FCA**

3. Regulatory imperative and scope

Regulatory perspective

It is important to understand the intention of the regulators and the drivers for issuing these publications.

This package of Consultation Papers and draft supervisory statements is a clear signal that going forward Operational Resilience will be scrutinised as much as financial resilience in the UK and will be embedded in the regulatory framework. The proposed policies will sit alongside other supervisory tools such as the senior managers' regime and S166 powers to request skilled persons' reviews.

The second point to note is the significance of the co-ordinated publication of these papers by the Bank of England, the PRA and the FCA. The joined-up approach and the fact that they have been published in an election "quiet period", when typically only the most important consultations are launched, underlines the importance the UK regulators attach to Operational Resilience as a long-term priority.

> "The proposals in the Consultation Papers make it clear that we expect you to understand your vulnerabilities, invest in protecting those and protecting yourselves, consumers and the market. We are confident that as a result of firms applying these concepts, customers will be better served by more resilient firms. This is why the proposals require firms to consider the impact of operational disruption with reference to each authorities' public interest objectives."
>
> **Megan Butler, FCA**

The key drivers of the proposals are the supervisory authorities' statutory objectives - the goal is a financial system that is resilient from front to back and can supply important business services with minimal interruptions, even during severe operational events.

From the UK regulators' perspectives, a more resilient system will deliver financial stability and consumer protection and promote more effective competition.

The regulators are pragmatic – they understand that operational disruptions will happen and that the goalposts are constantly moving. But lessons learned from a long list of previous failures, such as those set out in the Treasury Select Committee report in October 2019, show that there is still much that can be done to improve sector-wide resilience:

- Public perception and confidence that the system works will be critical to financial services firms as they move forward in a challenging environment.
- Firms that cannot clearly demonstrate resilience will lose business - and Boards and senior management will be held to account.
- Firms must prioritise the activities that could cause the greatest detriment to the system and its customers. They must clearly articulate what Operational Resilience looks like. And they must invest now to remain resilient in the future.

In her speech on 5 December, Megan Butler of the FCA referred to the need for a "shift in mind-set" – it is evident that these proposals are intended to drive change for individual firms and the wider financial sector. The regulators have made it very clear that they are expecting firms to focus on genuinely resilient outcomes, not just compliance with a set of rules.

The proposals in the papers are designed to build on and modernise the existing regulatory framework, and Financial Services firms will need to do more to anticipate further regulation.

UK scope

For the UK the scope of these proposals extends to the following groups:

- Banks, building societies and PRA-designated investment firms.
- Insurance and reinsurance firms and groups in scope of Solvency II.
- Solo-regulated FCA firms
- Branches of overseas banks and insurers (i.e. 3rd country branches).
- The outsourcing CP also contains proposals that are relevant to credit unions and non-directive firms (NDFs).

There are also specific Consultation Papers aimed at Central Counterparties, Central Securities Depositories and Payment Providers.

Global perspectives

It is also important to consider the global perspective:

- At European and global level, Operational Resilience is also a high priority.
- The UK proposals reflect guidelines already finalised by the EBA on Outsourcing arrangements, ICT and security risk management and EIOPA's draft guidelines on outsourcing to cloud service providers.
- And the FSB in Basel is engaged in the discussion around the financial stability implications of cloud and big tech.

Given the importance being given to Operational Resilience across the international regulatory environment, we would expect to see increasing collaboration in this space.

4. Important business services

It is apparent from the papers that the supervisory authorities have reaffirmed their intention to focus on the most important business services as a way of strengthening Operational Resilience and embedding of this concept within firms' operations.

> "Specifically, we expect firms and FMIs to identify their important business services. While we are not introducing a definitive list, we are providing further guidance on the type of business services that boards and senior management could classify as 'important'. We then expect firms to set an impact tolerance for each of these services, quantifying the maximum acceptable level of disruption through severe (or extreme in the case of FMIs) but plausible scenarios."
>
> **Building Operational Resilience: Impact tolerances for important business services**

External end user

The Consultation Papers provide a helpful clarification of what is deemed a business service –"a service that a firm provides to an external end user…. and delivers a specific outcome". It is also suggested that internal services (e.g. HR or payroll) should not be identified as business services. This may be different from the approaches we have observed at some firms which have designated some of these internal services as important business services and, therefore, may need to reflect changes going forward.

Critical chain of activities

A new addition since the Discussion Paper is the concept that firms should consider the chain of activities which make up a business service, and then determine which parts of that chain are critical to delivery and should, therefore, be resilient.

Clear definition has now been provided on the type of business services that should be classified as 'important'. These include business services which, if disrupted, could cause intolerable harm to consumers, the financial system and the firm itself. The potential to cause harm is a key concept in Operational Resilience. Example considerations for potential to cause harm are provided in the papers, such as the nature and size of the consumer base; substitutability, and the time criticality of the service.

In our experience, identification of important business services is one of the most significant milestones in an Operational Resilience programme, and sets both the scope and the implementation and business as usual (BAU) effort required. For this reason, additional guidance provided in the Consultation Papers should enable firms to validate and adapt their current approaches.

Proportionality and risk coverage

It is clear that identifying important business services will be a matter of judgement and will vary across firms depending on the firm's unique business model. The regulators expect firms to consider a range of risks when identifying their important business services, e.g. inability to make payments to the extent that financial stability is undermined, or to provide risk hedging services.

When determining the level of granularity for an important business service, firms should consider the following factors:

- Whether it allows for an impact tolerance to be applied which can be tested; and
- Whether it enables Boards and senior management to make prioritisation and investment decisions.

If the answer is "no" to these questions, then the service should be defined at a more granular level.

One of the frequently debated questions across firms is how many important business services there should be. There is no "magic number" or ballpark figure, as the number of important business services should be proportionate to the firm's size and complexity.

Trade-off: granularity, data availability, cost

Identification of important business services may be perceived as a complex, expensive and time-consuming effort, particularly in globally active, large firms. In our view, this will require a trade-off and a balancing act with the aim for firms to maintain as high a level as possible, whilst increasing granularity in specific areas to reflect sufficiently the "risk coverage" of the service. The level of granularity may not be consistent across different services that the firm provides to external beneficiaries, and that may be acceptable as the objective is to avoid insurmountable number of important business services due to associated cost and data points required, but nevertheless reflect nuances of service delivery. The key point is that firms must document their decisions to defining important business services in a clear, logical and auditable manner to withstand internal and regulatory scrutiny. For example, if firms are leveraging existing service or product taxonomies, they need to define design criteria against which the services are assessed and demonstrate how important business services are derived.

Firms should identify their important business services at least once a year or whenever there is a material change to their business or the environment in which they operate. Boards and senior management will be required to approve the important business services for their firm.

Prioritisation

Finally, the papers state that resilience of important business services should be prioritised over other business services. Prioritisation should inform investment decisions and direct appropriate allocation of resources to improve resilience.

5. Resource mapping

Mapping of resources, including third parties

Firms and FMIs are required to identify and document all resources (i.e. people, processes, technology, facilities, data and third parties) required to deliver each of their important business services. This is referred to as "mapping".

The new addition in the papers is the reference to including mapping of dependent processes. This is a welcome clarification that simplifies the development of service catalogues. Mapping will enable firms to understand the resources necessary to deliver important business services and to decide how to manage them to support service delivery in the event of disruption. Mapping can also facilitate understanding of dependencies and interconnectedness between services and operational resources underpinning those services.

> "We propose that firms should identify and document the resources that deliver and support their important business services. This is called mapping."
>
> **Megan Butler, FCA**

Focus on outcomes: vulnerabilities, mitigation, testing

The papers emphasise that mapping is intended to allow firms to produce certain specific outcomes:

- To identify vulnerabilities in delivery of important business services,
- Take mitigating actions to remedy vulnerabilities and
- Test their ability to remain within tolerances.

Examples of vulnerabilities include single points of failure, concentration risk, lack of resources' substitutability, dependencies on third-parties.

Mapping should be updated annually at a minimum or following significant change if sooner. Mapping needs to be complete, accurate, documented and signed-off at an appropriate level by management.

Trade-off: granularity, data availability, cost

As with the identification of important business services, mapping is not a prescriptive process and must be undertaken at the appropriate level of granularity as determined by each firm. There is no "one size fits all". Firms will need to develop their own mapping methodology that is proportionate to the size, scale and complexity of the business and the importance of the service, yet pragmatic and operable.

Existing approaches to mapping of resources to important business services vary across firms. In our experience, key considerations include:

- The firm's ambition – whether the firm is aiming to achieve compliance, resilience or service excellence; and
- The firm's choice in making trade-offs between the granularity of mapping and the insight achieved, and the quality and availability of data and resources the firm can invest in the process.

6. Outsourcing & third party risk

The consultation paper on outsourcing and third parties reaches broader and deeper than previous papers, having built upon the European Banking Authority (EBA) guidance in this space. However, EBA guidelines are only targeted at outsourcing arrangements, whereas the PRA paper extends to all third party arrangements, albeit that the majority of the in-depth requirements are still only for outsourcing.

> "We are concerned that these complex interdependencies increase the likelihood of a major disruptive event spreading quickly. It could be the failure of a shared piece of connectivity used in wholesale markets or loss of access to a major cloud provider. The types of solution we might expect to see more of include joined up engagement with these important suppliers by the authorised firms that rely on them, to properly understand those suppliers' resilience arrangements."
>
> **Megan Butler, FCA**

Board oversight of third parties

The paper clearly outlines that Board engagement is essential and the expectation is that the Board can appropriately identify and understand their firm's reliance on critical service providers and have appropriate strategies, systems and controls in place to manage them. The paper envisages the accountabilities for outsourcing being allocated to an appropriate SMF function(s) (usually SMF24 for most firms). The paper also gives guidance on the minimum standards for an effective outsourcing policy and includes examples of expected content.

Third party inventory, including cloud providers

Organisations will need to maintain an up-to-date register (inventory) of outsourcing relationships, distinguishing between those that are material and that are not. All Cloud outsourcing arrangements will need to be captured in a 'Cloud Register' (inventory). It is interesting is that the PRA is considering a standardized "Outsourcing Register" in a clear comparable format, which could provide a valuable tool for identification, monitoring and mapping of systemic third parties.

Third party materiality assessment, including systemic materiality

Organisations will need to define consistent assessment criteria to categorize the materiality of third parties based upon the role they perform in supporting important business services. (Note: The PRA is planning to introduce common criteria to improve consistency). It is a requirement to notify the regulators sufficiently in advance of outsourcing to a material service provider, rather than what has happened to date where some organisations have notified after the event.

Organisations will be required to assess the risks of all outsourcing arrangements irrespective of their materiality, considering financial and operational risks, and also taking into account any risks which the outsourcing arrangement may either mitigate, or help the firm manage more effectively.

Concentration risks (e.g., extensive reliance on one service provider) must be considered at a firm or group level, and risks associated with Cloud outsourcing managed, including both concentration risk and lack of substitutability, and firms must understand any tipping points for systemic risks arising from wider adoption.

Contractual arrangements (material outsourcing arrangements)

Firms will also need to include specific contract terms as required by the regulators, specifically for the following four areas:

- Data security;
- Access, audit and information rights;
- Sub-outsourcing; and
- Business continuity and exit plans.

Data security

According to the paper, data security, unlike for GDPR must apply not just to PPI data, but also to confidential, secret commercial and financial data). Organisations must define, document, and understand third parties' responsibilities with respect to data security, including:

- Data classification: Identifying data which firms would need to access and potentially migrate as a matter of priority in the event of disruption;
- Location of data: Adopting a risk-based approach to data location, considering data-at-rest, data-in-use and data-in-transit (e.g., encryption and key management, identity and access management, and incident detection and response); and
- Outsourcing policy: Implementing appropriate measures to protect outsourced data set out in the outsourcing policy and in written agreements.

Access, audit, and information rights

Firms must ensure that material outsourcing agreements provide the firm and regulators with unrestricted access, audit and information rights covering (as appropriate):

- Premises;
- Data;
- Devices;
- Information; and
- Systems, and networks

Additionally, the PRA is emphasizing "pooled audits": audits organized by groups of firms sharing one or more service providers (or facilitated by the service providers) and performed by representatives of the participating firms, or by specialists appointed on their behalf.

Sub-outsourcing

Where material outsourcing arrangements involve sub-contracting, organisations must:

- Maintain up-to-date lists of entities they sub-contract;
- Pay attention to the potential impact of large, complex chains of sub-contracting service providers on their Operational Resilience (e.g. in the end-to-end provision of important business services); and
- Specify in written agreements whether sub-contracting is allowed and, if so subject to what conditions.

Business continuity, exit plans and testing

Firms must develop, document and test robust business continuity plans and exit strategies to improve the firm's ability to withstand and recover from potential failures and outages of material third party service providers. For each material outsourcing arrangement, firms should develop, document, and retain a business continuity plan with the following characteristics:

- Developed to anticipate, withstand, respond to and recover from severe but plausible disruption;
- Considering factors including cloud resiliency and destructive cyber-attacks;
- Ensuring effective crisis communication to all stakeholders;
- Developed in the pre-outsourcing phase;
- Assigning clear roles and responsibilities; and
- Developed and executed by multi-disciplinary teams.

Firms should differentiate situations where a firm exits an outsourcing agreement due to:

- Stressed exit: Caused by disruption, an outage or the failure (i.e., insolvency or liquidation) of the service provider); or
- Non-stressed exit: For commercial, performance or strategic reasons in a planned and managed way.

For cloud providers, firms should develop a 'Cloud resiliency' plan (e.g. leveraging the resilience of multiple availability zones, regions, or service providers).

7. Impact tolerances

Risk appetite vs impact tolerance

One of the areas where additional clarity and guidance was requested through feedback on the Discussion Paper was impact tolerances. The Consultation Papers provided clear definition for what an impact tolerance is, as well as clarifying the difference between impact tolerance and risk appetite. The guidance provided is that a risk appetite statement articulates the amount of risk a firm is willing to take in pursuit of its strategic objectives, whereas an impact tolerance assumes that a particular risk has already crystallised and articulates the maximum tolerable level of disruption for that risk.

> "Firms and FMIs are responsible for setting their own tolerances, and boards and senior management should take actions to improve Operational Resilience where limitations are identified in a firm's or FMI's ability to remain within these tolerances. This is where firms and FMIs should expect close supervisory scrutiny and engagement."
>
> **Building Operational Resilience: Impact tolerances for important business services**

Expectation that time will be one metric

The papers have also provided further guidance on the metrics that firms should use, in order to measure impact tolerances. They have been explicit in setting an expectation that all firms should use time as one of the metrics, but also suggested that other metrics can be reported including value and volume.

Demonstrate decisive and effective actions

Firms will also be required to demonstrate that Senior Management and the Board are taking decisive and effective actions to remain within impact tolerances. Where this is not the case, firms will be expected to articulate what actions they are taking to remediate these known issues, for example replacing outdated systems, increasing system capacity, etc.

Multiple metrics for dual regulated firms

For those firms that are dual-regulated, there is also an expectation that impact tolerances will need to articulate how they have considered risks associated with financial stability and safety and soundness as well as consumer harm and harm to market integrity.

There is an expectation that firms will be able to demonstrate that they are able to remain within their impact tolerances, no later than 3 years after the rules come into effect. Firms therefore need to immediately start to think about their approach and method for defining and setting impact tolerances, as well as designing the scenarios against which they will be tested.

Firms should consider that they are not expected to resume the provision of an important business service within the impact tolerance, if the risk associated with the cause of the failure still remains – for example in malware attacks.

Impact tolerances should be primarily used as a planning tool, to identify where investment is required and where suitable workarounds/substitutes are needed for those scenarios where a firm will be unable to recover within the tolerance that has been set.

8. Scenario definition and testing

The Regulators have used the papers to further highlight the importance of identifying severe, but plausible scenarios that can be used to assess whether the firm can resume the delivery of an important business service within the impact tolerance.

Failures within and outside the firm's control

Scenarios should include failures where the cause is both within and outside of the firm's control, acknowledging that incidents such as a network power outage or failure of a piece of core market infrastructure are definitely plausible scenarios, and the papers have stressed the importance of identifying both availability and data integrity-based scenarios. Scenarios should cover a broad range of adverse circumstances and the papers have also advised that firms should not make the probability of a certain scenario occurring one of the key determinants of plausibility.

> "Testing your ability to remain within your impact tolerance, during a severe event, is likely to reveal gaps and weak points in the resources that support delivery of the important business service. Used properly, testing your ability to remain within your impact tolerance should lead firms to taking actions that make a real difference to your Operational Resilience."
>
> **Megan Butler, FCA**

Co-testing with third parties

The papers have provided additional guidance on the level of testing required, and have emphasised the importance of co-testing with third parties. Differing types of testing are also suggested, ranging from simply analysing data from previous incidents, through to desktop based scenarios and even live testing in some instances.

The importance of conducting lessons learned exercises is re-iterated in the papers. The principal objective is to ensure that prioritised investment decisions are made for the most important business services to ensure they have the ability to recover and respond from operational disruptions.

Communications plans

Robust communications plans are highlighted as a key requirement under Operational Resilience. These plans should articulate how both internal and external communications will take place during a crisis. This should ensure that internal stakeholders are aligned with actions being taken and external customers or counterparties are clear on the status of the disruption and the alternatives available to them.

KPMG considers that the severity of most firms' testing plans, and the frequency of tests currently being conducted, do not meet the proposals articulated in the papers. Firms will need to be able to demonstrate a much more rigorous schedule of severe, but plausible scenario tests across their portfolio of important business services. Scenarios should include both internal and external causal factors and cover incidents where the root cause is broader than simply asset availability issues, and firms should ensure that 3rd parties are active participants in fully simulated scenario tests.

9. Delivering Operational Resilience

Impact tolerances as a planning tool

This is a new concept that articulates how firms will be expected to demonstrate that they have taken decisive and effective actions to improve their organisation's level of resilience. Impact tolerances are just one example of tools that the regulators will expect firms to use in order to ensure that appropriate investment decisions are made and that important business services can be recovered within tolerance.

> "Operational risk management is not infallible. In risk management, you can assume harm will occur and still be comfortable so long as you are able to stay within your agreed risk appetite. Operational resilience on the other hand is an outcome. It is a step change, where we expect you to be forward looking and making decisions today that help prevent harm tomorrow."
>
> **Megan Butler, FCA**

Reference is made to the fact that resilience will need to have tangible links to existing policies, such as operational risk, as well as to the traditional business continuity and IT disaster recovery functions. There is therefore a clear expectation that, in future, Operational Resilience will play a major role in the operational risk management of an organisation.

Self-assessment

It is clear that the emphasis on Operational Resilience is here to stay and that this cannot be just a one-off exercise. Firms will be required to embed a repeatable set of processes as part of a broader operating model within their organisation. They will also need to be able to demonstrate the ability to produce, upon request, self-assessment documents that articulate the firm's important business services and associated impact tolerances, a testing schedule based upon severe, but plausible scenarios, and awareness of known vulnerabilities that threaten the firm's important business services and therefore the current level of resilience across the organisation.

SMF 24 accountability

There is also an acknowledgement that the SMF 24 function is the one most likely to be made accountable for Operational Resilience. For those firms where this function does not exist, it will be necessary to determine the most appropriate individual within the firm to be accountable for resilience.

Prioritise actions based on risk

Senior Management or Boards will need to be able to demonstrate that they are prioritising the remediation of resilience deficiencies associated with important business services, and in particular those that may pose a significant risk to financial stability. Boards will also be required to review and approve the self-assessment documentation on a regular basis, and more frequently, when there are changes to the firm's operating model, business strategy or global footprint.

10. Practical considerations

> "We believe that, in the public interest, a resilient financial system should always aim to supply its important business services with minimal interruption even during severe operational events. It's the resilience outcome that's most important to the supervisory authorities, not simply a firm's ability to demonstrate compliance."
>
> **Megan Butler, FCA**

KPMG has identified some practical recommendations relating to where firms can enhance the business case and drive value as they set-out on the journey ahead:

1. Our client work has clearly demonstrated the benefits of considering the complete operating model, looking at governance, organisation, processes, data, and tooling from the outset and in all of your pilots.
2. Starting with a broad perspective will allow the real opportunities and challenges to be identified early on in the process so that practical and workable solutions can be developed, proven and scaled. The following points identify some of the key considerations:
    a. Thinking about the whole organisation, the pilots need to answer key questions:
        i. How will the 1st and 2nd line interact;
        ii. How will existing functional roles evolve; and
        iii. How will the organisation need to change to develop a healthy tension between horizontal service accountability and the respective resource owners?
    b. For governance:
        i. How will we effectively integrate Operational Resilience within our Operational and Enterprise-wide risk frameworks?
        ii. How do we best align and repurpose existing governance fora and reporting?
    c. What are the resilience processes that a "Chief Resiliency Officer" will need to be in place to ensure a continuous and comprehensive focus on the firm's resilience?
    d. KPMG advocates re-using and adapting what firms have in place today.

There are two areas to which KPMG believes firms must give particular consideration early on in the implementation journey:

1. First, the relationship between Service Management & Operational Resilience. These are not one and the same, and firms that decouple service management from the resilience operating model can drive broader benefits, across areas such as cost, performance, risk and transformation from the consistent and granular understanding of the firm's service delivery model.
2. Second, Data and tooling – practical experience has shown us that data quality and availability and the associated tooling are key to the scaling and sustainability of the resilience operating model and its business case.

To conclude, we now believe that firms have the green light to move forward with confidence, but should take care to ensure that their plans place proper emphasis on the scalability and sustainability of solutions.

KPMG Operational Resilience contacts

Below is a list of some of our Operational Resilience subject-matter experts. Please reach out to any of them if you have any questions arising from this report, or from the Consultation Papers themselves.

Andrew Husband
Partner

Operational Resilience Financial Services Lead
E: andrew.husband@kpmg.co.uk
T: +44 207 6941040

Lulu O'Leary
Partner

Operational Resilience Insurance Lead
E: lulu.oleary@kpmg.co.uk
T: +44 207 6943105

Scott Lee
Director

Operational Resilience Wealth & Asset Management Lead
E: soleary,cott.lee@kpmg.co.uk
T: +44 141 3092085

Douglas Dick
Director

Operational Resilience Third Party & Cloud Lead
E: douglas.dick@kpmg.co.uk
T: +44 207 6943767

Ashley Harris
Director

Operational Resilience Banking Lead
E: ashley.harris@kpmg.co.uk
T: +44 207 6942913

Marija Devic
Director

Operational Resilience Wholesale Banking Lead
E: marija.devic@kpmg.co.uk
T: +44 207 3114451

kpmg.com/uk

Designed by CREATE | CRT112863