Operational risk and operational resilience

pwc

Call to action

Heads of operational resilience

1

should look at how parts of the firm's existing risk, process and controls architecture can help them to accelerate the design and implementation of their approach to meet the new operational resilience policy regime and also prevent unnecessary duplication. Insights from operational risk will be vital in ensuring the operational resilience of important business services and of the organisation as a whole.

Important business service owners

2

should build a clear understanding of the end-to-end delivery of their service. This involves leveraging what already exists (e.g. process maps) and developing forward-looking indicators, aligned to impact tolerances, to support monitoring of operational resilience and decisive management action. They will need to understand the risks and controls embedded in their end-to-end process in order to do so.

Heads of operational risk

3

should use operational resilience insights to drive further value and benefits to the organisation from enhanced operational risk management. This information can also provide an opportunity to assess whether existing infrastructure and methods are delivering the right outcomes for their organisations.

Making the whole greater than the sum of its parts

The ever-increasing focus on operational resilience has provided firms with an opportunity to look at their organisations with fresh eyes and kick the tyres on their existing approaches to understanding and responding to what could go wrong. Becoming resilient will require more than simply continuing to perform existing risk management practices. However, this does not mean that firms have to start from scratch.

Many firms are rightly looking to understand what they can leverage from their existing frameworks and infrastructure. In our recent publication, **'Becoming operationally resilient: Preparing for new UK policies**[1]', we suggest that those firms which are more advanced in their implementation of the new operational resilience policies should actively look at the roles and responsibilities across all three lines of defence as well as the use of existing tools. For instance, operational risk management frameworks can offer tools such as impact scales and scenario testing templates that can accelerate progress in meeting new policy requirements while giving confidence that the underlying risks are in control. Being able to piggy-back on these established tools and insights can save valuable resources and prevent duplication or inefficiencies being created. **Perhaps the greatest opportunities, though, come through the ongoing monitoring, response and governance of both disciplines**.

This can also be an issue of timing. In the longer term we would expect there to be strong links emerging between the way that firms manage risks and the way they manage the (operational) resilience of their most important services. However, in the short term, we are finding that firms are focused on making swift and demonstrable progress on building their resilience frameworks and identifying and mapping important business services and tolerances, rather than investing in activities to drive greater alignment.

This paper explores how resilience and risk practitioners could work together to leverage their respective disciplines.

[1] https://www.pwc.co.uk/industries/financial-services/regulation/understanding-regulatory-developments/becoming-operationally-resilient-preparing-new-uk-policies.html

Context

BCBS papers on operational risk[2] and operational resilience[3] define the terms as follows:

'Operational risk is defined in the capital framework as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.'

'Operational resilience is defined as the ability of a bank to deliver critical operations through disruption.'

The 2020 BCBS consultation on the principles for operational resilience looks to get firms to focus on the right activities and behaviours to drive towards an ambition of greater operational resilience:

'Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience approach.'

In a 2020 blog[4] we drew the analogy with healthy living when considering operational risks. For instance, most of us know we should eat right and stay active, but this has not prevented the obesity crisis facing society. By doing the right thing, we build our personal resilience. As a result, guidance has become more specific and more directive, such as through colour-coded food labels and gadgets to monitor our (in) activity, with recommendations on what exercise to do. We know what to do, and yet we don't do it. Similarly, with operational risk management the concepts are simple – in that firms need to understand what they do, what could go wrong, how to stop things from going wrong, and how to respond when they do. Yet evidence suggests[5] that many firms haven't achieved this in practice.

Regulatory focus on operational risk

Over the last 18 months regulators and standard-setting forums have been more active in clarifying expectations for operational risk management, both through published guidance such as the Basel Committee's Principles of Sound Operational Risk Management, as well as through supervisory reviews of firms. Our experience in the market has highlighted several recurring themes that firms are being asked to address to improve their operational risk management outcomes.

Cohesion of approach to managing operational risk

Regulators have been raising concerns around situations where boards and senior management lack a clear line of sight into operational risk exposures, often due to ineffective risk framework implementation. This includes:

- how risk management integrates with other business processes (e.g. new product approval), to ensure that risks are identified, managed and monitored appropriately through the lifecycle;
- a lack of alignment between framework elements (e.g. scenario analysis not feeding into control investment decisions) and risk types (e.g. management of technology risk and third party risk operating in silos); and
- inaccurate and/or incomplete views of risk profiles at both an individual business line level and aggregate basis across the organisation, preventing an end-to-end view of the threats faced.

Data quality and data governance

Effective data quality management continues to be a key priority. Regulatory inquiries in this area highlight a need for organisations to develop a comprehensive data governance framework and allocate appropriate resources to deliver and oversee it. The pervasiveness of data and the importance of data security mean firms should ensure that all staff have at least basic skills to manage data quality well, and to derive insight into the business and its risks. After all, how can the firm generate the right insight into its business and related risks without good, and well-managed, data.

Incentivising risk management

Individual firms and regulators have recognised the impact that a well-calibrated performance management programme can have on enterprise-wide risk management. As an example, a public consent order issued by the US regulator (OCC) highlighted that the failure of compensation and performance management programmes to incentivise effective risk management constituted an 'unsafe practice'. Our own experience from supporting risk management enhancement programmes has shown that firms consider performance management a key tool for embedding good risk behaviours.

[2] https://www.bis.org/bcbs/publ/d515.htm

[3] https://www.bis.org/bcbs/publ/d516.htm

[4] https://pwc.blogs.com/fsrr/2020/08/basel-committee-serves-up-a-healthy-dose-of-operational-risk-management.html

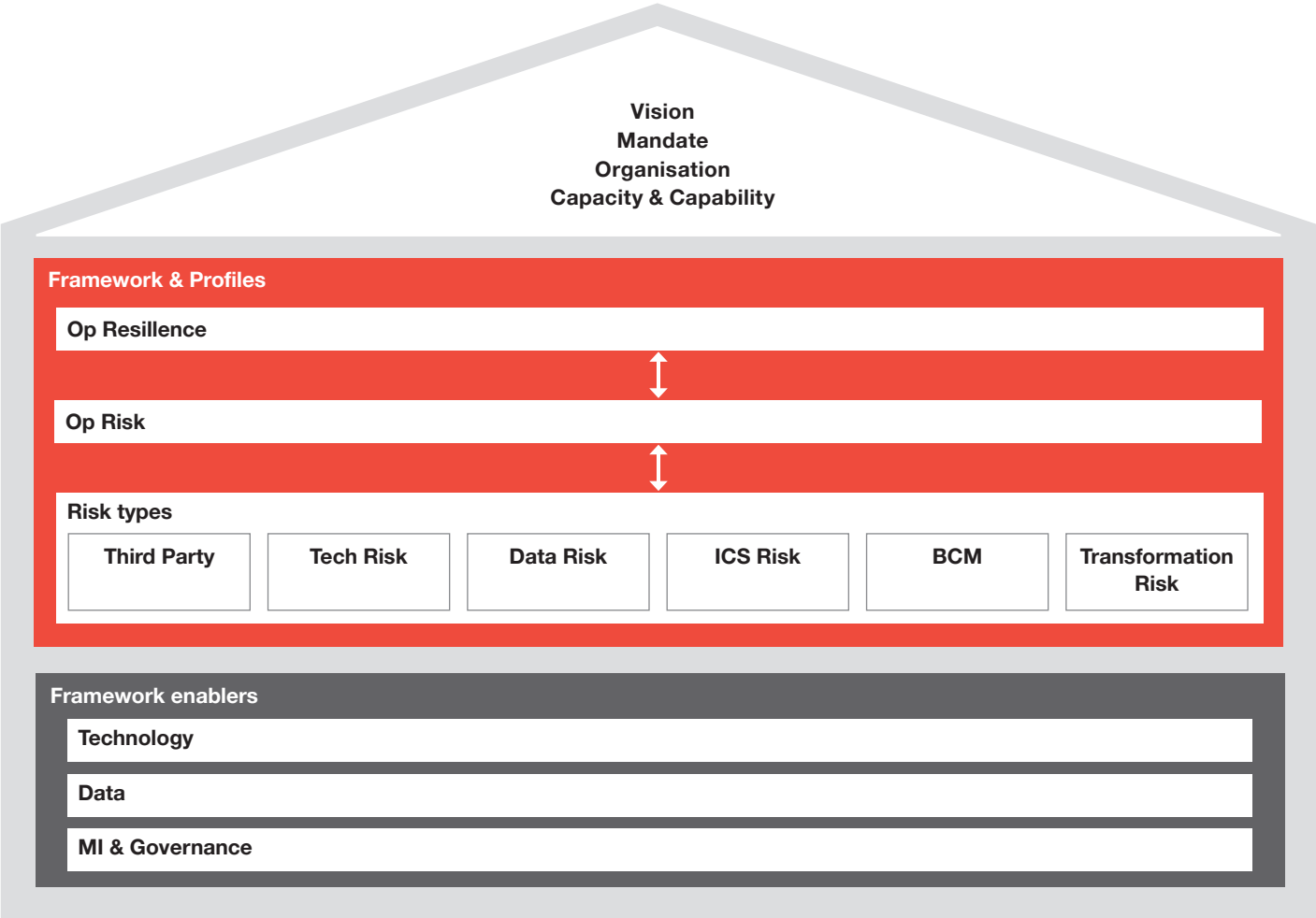
[5] A **European Banking Authority report** highlighted the poor state of operational risk management within European banks, finding that only one in ten SREP (Supervisory Review and Evaluation Process) reviews considered operational risk management to be 'good' (i.e. rated 1 or 2 out of 4) compared with around 60% for Credit Risk and 80% for Market Risk.

Bringing operational risk and operational resilience together

Those leading operational resilience programmes at firms are not necessarily those with existing responsibilities for risk management. They should look at how parts of the firm's existing risk architecture can help them to accelerate the design and implementation of their approach and also prevent unnecessary duplication. In most instances existing operational risk infrastructure will not, on its own, enable firms to achieve compliance; rather, operational risk provides a starting point or input to enable firms to build from an existing base.

How resilience can sit within the risk management architecture

The below figure outlines how operational resilience can sit within the existing non-financial risk operating model. The operating model includes both Line 1 and Line 2's vision, organisational structure and capabilities as well as the common technology, data and governance leveraged by both lines of defence. This integration enables operational resilience to use what already exists; however, it also means that the effectiveness of operational resilience is dependent on the efficacy of the existing risk architecture. In the figure below the minimum requirements of third party, technology, data, information and cybersecurity, business continuity management (BCM) and transformation risk are all aligned to the minimum requirements articulated in the operational risk framework (increasingly referred to as the non-financial risk framework). This enables a consistent approach to be taken to the risk management cycle which can then be leveraged, and enhanced, by operational resilience practitioners. Conversely, inconsistent approaches to these risk types may make it more difficult for operational resilience to leverage what already exists, without first enhancing and streamlining risk infrastructure.



How your approach to operational risk can help you to become resilient more efficiently

Those who are looking to build out and implement your firm's approach to operational resilience can use operational risk tools, templates and outputs to leverage existing practices and avoid reinventing the wheel. The below table outlines some potential synergies that can be made between elements of both the operational risk and resilience cycles.

	Operational resilience practitioners must	Operational risk tools which can be leveraged
Identifying important business services (IBS)	Identify the firm's important business services which are those where disruption could have an intolerable impact on consumers, the market or the firm itself	• Risk assessments setting out the level of inherent risk (e.g. conduct and market) can be used as an input into the determination of an IBS. These risk assessments will likely be by business unit or product line and will need to be 'connected' to a business service
Mapping	Identify and document the processes which make up the important business service and the people, third parties, technology, facilities and data needed to deliver each one	• Firms that have process-led risk and control self assessments (RCSAs), require a consistent catalogue of key processes to drive this assessment. Where these are service-oriented processes, they can be leveraged to string together the end-to-end view of an IBS and its vulnerabilities • If not already included in the above, firms should link to registers of outsourcing arrangements (including sub-outsourcing arrangements) and technology assets (see call-out box below for further information)
Impact tolerances	Set an impact tolerance which represents the maximum tolerable level of disruption to an important business service	• Firms can leverage the impact scale/matrix being used for risk assessments currently (though this will often need to be expanded to include additional impact consideration for consumers and markets) • Potential to use the firm's risk appetite as an input/review point to the setting of the impact tolerance thresholds (please see call-out box below for further information)
Scenario testing (including lessons learned exercise)	Test the firm's ability to remain within impact tolerances for severe but plausible scenarios. Conduct a 'lessons learned' exercise to enable the firm to identify weaknesses and take action to improve its ability to effectively respond and recover from future disruptions	• Leverage existing scenario testing templates and methodologies • Adapt existing scenarios to support testing of disruption to IBS • Leverage work done to identify drivers and causes of risk events. This can include trends from Key Risk Indicators as well as taking the causes recorded in RCSAs to understand the potential vulnerabilities along the end-to-end process
Lessons learned/ Response to remain within impact tolerances	Where the business service would not be able to remain within impact tolerances under severe but plausible scenarios, develop and implement effective remediation plans for the IBS	• Consider where potential control enhancements have already been identified or where action plans are already in place to reduce the probability or impact of these risk events occurring • Use existing governance (e.g. central issue logs) to ensure adequate oversight of these
Self assessment	Maintain a written record of the firm's assessment of its compliance with the operational resilience policies	• Use existing attestation approaches to get input from business service owners into the resilience of their services

Mapping of important business services

The mapping of important business services is seen as a valuable exercise by firms as it drives a deeper understanding of their delivery models and dependencies on core resources. However, the activity to prepare the initial maps and then develop an effective way to maintain them often brings significant challenges to firms. Many firms already have databases covering their technology assets and third party relationships, for instance, but without a tool to link these to the processes they support and ultimately to a business service view. Identifying a single tool to bring these pieces of information together would make it easier for firms to manage updates to this view and give them greater confidence in the integrity of the data over time.

Aligning risk appetite to impact tolerances:

The ability to align risk appetite to impact tolerances is dependent on two things:

- How well firms have articulated their existing risk appetite related to disruption, i.e. recovery time and impact, and how this has been cascaded into the firm's risk assessment and management activities for individual risk subtypes e.g. third party, information security risk; and
- How well the existing risk appetite has then been cascaded into business units or functions.

However, in practice many firms have not articulated their non-financial risk appetite with sufficient clarity for businesses to know when they are in and outside of appetite, including those related to disruption. Firms have also often found it difficult to cascade appetite to individual business lines and functions; and only manage to appetite at a group-level. In these instances utilising appetite to inform impact tolerances becomes difficult.

Ongoing monitoring and governance

While ongoing monitoring does not form part of the additional rules and guidance within the new UK operational resilience regime we would expect firms to have developed regular monitoring and governance mechanisms to enable oversight over the firm's ability to 'prevent, adapt, respond to, recover and learn from operational disruptions'. This would fall in line with existing broad supervisory expectations about how a firm conducts its affairs and manages its risks.

Rather than create new monitoring and governance mechanisms, we would imagine most firms should first seek to review and, where possible, enhance what is already in place to enable resilience outcomes. This will prevent firms from further clogging the diaries of senior management with additional governance commitments and can act as a burning platform to enhance the effectiveness of existing forums.

From a reporting perspective, firms are considering whether to adjust existing MI to include consideration of resilience outcomes or the creation of resilience-specific MI. The firms that are creating resilience-specific MI are doing so to ensure there is adequate consideration of resilience in management oversight and decision making, particularly where existing governance forums are being utilised. Similarly, resilience may result in service-led MI being created in addition to, or instead of, functional MI. Regardless of the approach taken, system and data requirements will need to be updated to align with the new MI requirements.

How your approach to operational resilience can help you to manage your operational risk more effectively

Those who own or implement operational risk frameworks can also use operational resilience to help them to focus on what really matters to their organisation. It can also provide an opportunity to assess whether existing infrastructure and methods are delivering the right outcomes for their organisations[6].

	Operational risk requirements	Operational resilience insights which can be leveraged
Risk-based focus	Operational risk practitioners in both line one and line two should focus on those areas which are most critical to their firm (e.g. increasing or largest risk exposure)	Looking at the business through an operational resilience (or important business service) lens will enable senior management to focus on what is most critical to their business. It is also likely that regulators will be increasingly interested in how IBSs are being managed from a BAU perspective and may well feed into the scoping of regulatory reviews
Risk identification	Business Lines need to identify all risks generated by their business activities; not just those that they directly control	A full end-to-end view of an important business service will highlight for many businesses what they rely upon in order to perform their business activities that may have been missing in their risk profiles to date, as well as interdependencies between IBSs themselves. For example, a view of the technology and third parties utilised by the IBS, what risks they generate/change and the controls used to mitigate those risks. Note, this goes beyond the current inclusion of technology and third party risks in their profiles and requires them to reference, for example, what data access controls are in place in the third parties to help control information security risks
Risk assessment	Business lines should develop a full understanding of the different impacts a risk crystallisation could have in both a BAU and severe but plausible context. This includes the identification and assessment of all controls which help to manage the risk, with adequate alignment between control design and operating effectiveness, and a clear articulation of residual risk exposures	Further insights can be gleaned from the broadening of impact considerations (e.g. broader customer impact such as financial loss to clients, market or consumer confidence, spread of risks to other business services, other firms or UK financial system, data confidentiality, integrity and availability). There is also the potential for enhanced alignment between stress testing results and BAU investments in control and appetite
Risk mitigation	Risk mitigation actions should be proportionate to the risk exposure being mitigated	A more holistic view of impacts enables risk mitigation investments to be more targeted on what matters most. Furthermore, operational resilience forces firms to revisit the interconnected elements of their frameworks; for example, the outcomes of scenario analysis feeding into control mitigation investments
Risk monitoring	Risk monitoring should enable a forward looking view of risk profile changes and control effectiveness	This is a prompt for IBS owners to develop forward-looking indicators, aligned to impact tolerances that are actively monitored by business services. It can also be an opportunity for existing Key Risk Indicators and Key Control Indicators to be reviewed and uplifted, and to increase the alignment between these monitors and management action
Risk response	Consistent approach to the way that issues and incidents are responded to by the organisation	If not done already, a consistent approach to risk, BCM, operational resilience etc. can enable efficiencies to be created and response channels be more easily understood across the business

[6] Principle 6 of the revised principles for the sound management of operational risk now includes more detailed examples of tools used for identifying and assessing operational risk.

Third party risk management

In recent years we have seen the emergence of cloud technology and the continued growth in the scale and complexity of firms' third party dependencies. This has been reflected in significant updates to regulatory frameworks for outsourcing and third party risk management. These continue to emphasise that firms remain fully accountable for their outsourcing arrangements and managing these and all third party arrangements proportionate to the risks they present.

This increasing emphasis on broader third party risk management is now extending to more explicit linkage to operational resilience; particularly so in the UK, where the PRA's implementation of the EBA Outsourcing Guidelines fully integrates their broader operational resilience objectives[7].

Under the new UK operational resilience policy firms must map the process steps and underlying resources needed to deliver their important business services, including those resources which are delivered by third parties, both intra-group or external. Firms will use these maps to identify vulnerabilities in their current delivery models and use severe but plausible scenarios to test their ability to remain within defined impact tolerances using an appropriate response. These scenarios could include incidents involving disruption to a third party service provider's operations or the leakage or theft of sensitive information from a third party.

Regulators will tend to be agnostic of how the service is delivered as long as it can be demonstrated that the risks are being managed proportionately, and subject to appropriate senior management control and oversight. Therefore they will expect firms to have conducted thorough risk assessments to understand and quantify the nature and extent of risks throughout the chain, understanding that threat actors will look to exploit the weakest links within these. Similarly the expectations are that these risks are understood at both the arrangement and aggregate level, managing any concentration risks.

Regulators will also expect firms to consider substitutability of third party providers and interrogate exit strategies and plans to gain assurance that a firm is able to maintain delivery of important business services, particularly in the event of a stressed exit.

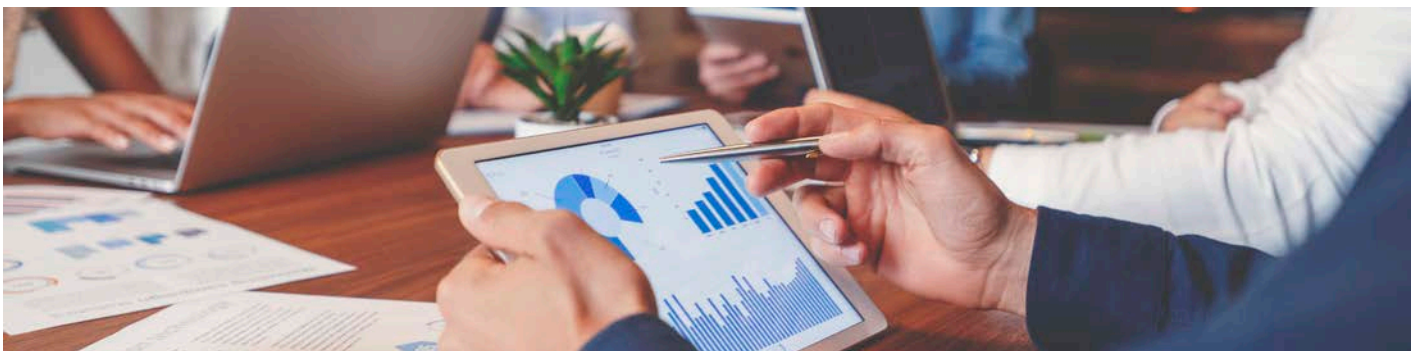
> "The technical complexity of some technologies provided by third parties coupled with the fact that they are constantly evolving can make it difficult for firms' boards and senior management to understand and manage relevant risks.
>
> Source: PRA CP30/19 Outsourcing and third party risk management

Third party risk management cycles will consist of the following steps:

- Risk identification, assessment and due diligence
- Approvals and notifications
- Contracting
- Migration
- Monitoring and oversight
- Change management and exit

Drawing upon operational resilience insight can support the steps in the lifecycle through, for instance, a better understanding of how the third party service fits into any important business service, informing contractual terms with the third party provider, and establishing expectations on scenario testing and exit plan testing.

[7] https://www.pwc.co.uk/industries/financial-services/regulation/understanding-regulatory-developments/outsourcing-and-third-party-risk.html



How PwC has helped our clients

Case study – banking sector

We have been working with a banking client on leveraging its evolving operational resilience approach to enhance its operational risk framework, and vice versa. Like many firms it recently established a programme to address evolving regulatory requirements related to operational resilience. While this helped the firm to accelerate its understanding of the requirements and to pilot its approach, it was also identified that continuing to develop new infrastructure in a vacuum may duplicate effort and/or create multiple versions of the truth.

PwC was brought in to assist the firm to review how existing tools and requirements within the operational risk framework could be better leveraged to create a more consistent and effective approach to operational resilience. This included a review of risk appetite, scenarios, risk and control identification and assessment, responses (including escalation and governance), interactions and documentation.

This work highlighted that existing operational risk infrastructure could indeed be leveraged to assist the firm in meeting operational resilience requirements across the full operational resilience cycle. However, it also highlighted where potential enhancements could be made to existing operational risk practices to align with evolving regulatory expectations.

Finally, this work demonstrated that in some instances the full integration would not be able to take place in the short term without compromising operational resilience delivery timeline for the target end-date of 2021. However, understanding the end-state enabled the firm to work towards a more integrated state and plan out the continued enhancement of operational risk management activities alongside resilience activities.

Contacts

Rakesh Majithia
Partner, Resilience & Risk Management Lead
M: +44 (0)7803 023856
E: rakesh.majithia@pwc.com

Paul Atkinson
Partner, Resilience & Risk Management
M: +44 (0)7764 958656
E: paul.j.atkinson@pwc.com

Symon Dawson
Partner, Risk Transformation
T: +44 (0)20 7804 1225
E: symon.k.dawson@pwc.com

Jess Sparksman
Director, Operational Risk
M: +44 (0)7843 332449
E: jessica.sparksman@pwc.com

Charles Rodger
DIrector, Third Party Risk Management
M: +44 (0)7884 317642
E: charles.m.rodger@pwc.com

Kelechi Igboko
Director, Operational Resilience
M: +44 (0)7802 659045
E: kelechi.v.igboko@pwc.com

Adam Stage
Senior Manager, Operational Resilience
M: +44 (0)7483 422845
E: adam.stage@pwc.com

2021-02-17_RITM4677058