THE INVESTMENT ASSOCIATION

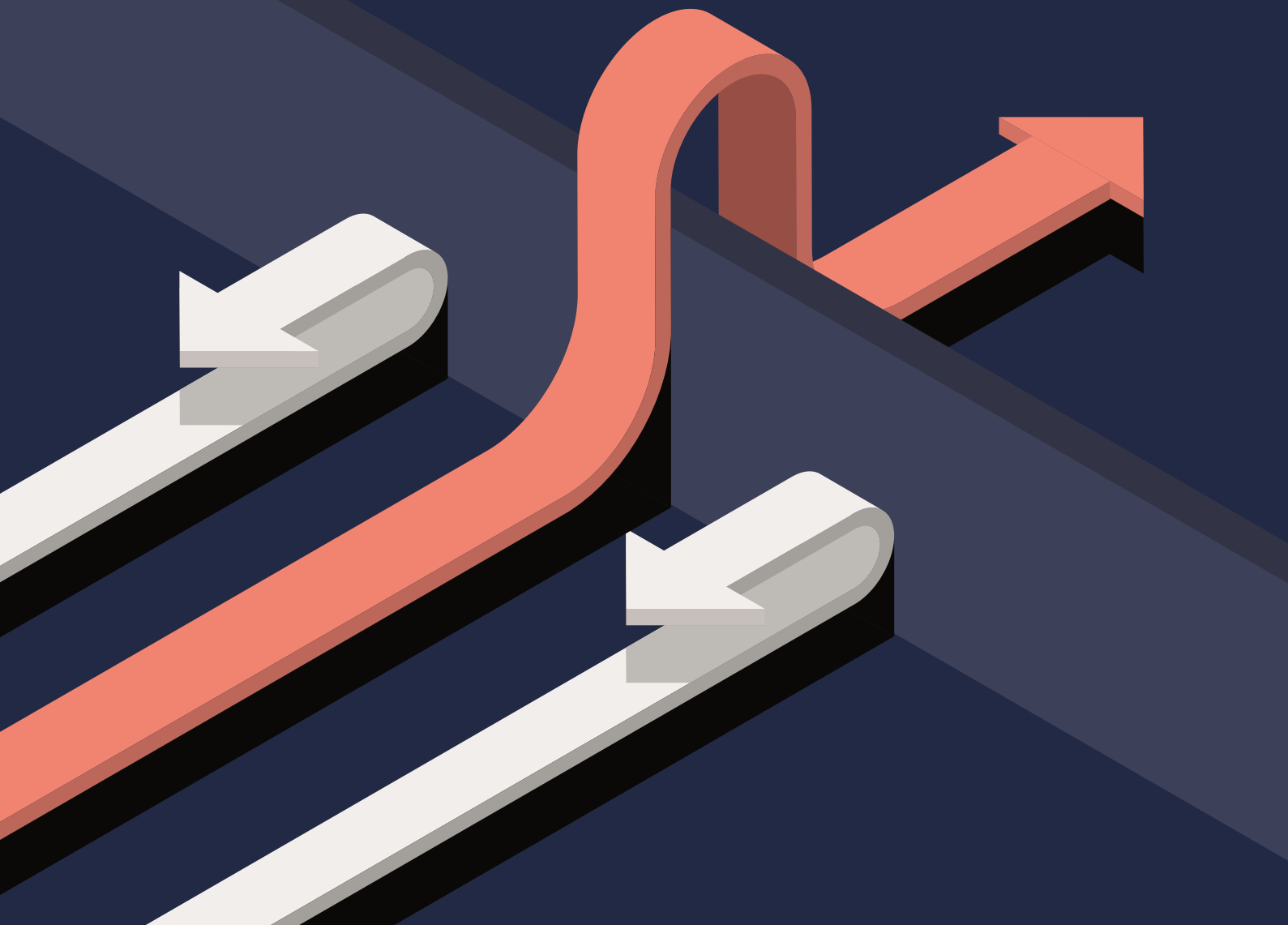
In collaboration with

EY
Building a better working world

EFFECTIVE GOVERNANCE

of Operational Resilience

February 2021



About the IA

The IA champions UK investment management, supporting British savers, investors and businesses. Our 250 members manage £8.5 trillion of assets and the investment management industry supports 113,000 jobs across the UK.

Our mission is to make investment better. Better for clients, so they achieve their financial goals. Better for companies, so they get the capital they need to grow. And better for the economy, so everyone prospers.

Our purpose is to ensure investment managers are in the best possible position to:

- Build people's resilience to financial adversity
- Help people achieve their financial aspirations
- Enable people to maintain a decent standard of living as they grow older
- Contribute to economic growth through the efficient allocation of capital

The money our members manage is in a wide variety of investment vehicles including authorised investment funds, pension funds and stocks and shares ISAs.

The UK is the second largest investment management centre in the world, after the US and manages over a third (37%) of all assets managed in Europe.

About EY

In our wealth and asset management work today, not everything is innovation; a lot of it is evolution. And it's important to know the difference. FinTech disruptors continue to shift the rules, newer investors aren't flocking to older channels and cost pressure is relentless. From data and AI, to tech platforms and partners, the questions have never been bigger, and the stakes have never been higher.

At EY, we help clients re-think everything from pricing and operating models to coopetition and convergence. We bring critical questions into focus, which lead to bolder strategies, simplified operations and sustainable growth. Our sharp understanding of the state of play allows us to shift discussion from reacting to change, to helping shape it. Ultimately, we work with clients not just to stay competitive, but to change investing for the better.

CONTENTS

FOREWORD

PAULINE HAWKES-BUNYAN

DIRECTOR, BUSINESS: RISK, CULTURE & RESILIENCE AT THE INVESTMENT ASSOCIATION

To ensure effective operational resilience, having the appropriate people and processes in place to govern a firm's strategy is undeniably crucial.

Following the publication of the draft operational resilience proposals by the UK regulators, the Investment Association (IA) in collaboration with EY convened a working group looking at operational resilience governance arrangements and how to produce effective management information (MI).

This report highlights a range of potential approaches members can take when considering their operational resilience governance arrangements.

The COVID-19 pandemic and the rapid transition to remote working has placed operational resilience directly in the spotlight. Our industry has remained resilient in face of this test of a 'severe but plausible' scenario and also identified those individuals responsible for implementing an operational resilience strategy. However, the message from the regulators is that the work does not end here. It is more apparent than ever that having a clear tone from the top can help embed a culture of resilience across an organisation.

Cultivating and maintaining a healthy culture continues to be a priority for the industry and the IA remains dedicated to supporting members in this area. Those who had been focused on fostering a healthy culture prior to the pandemic informed us that this had helped them to successfully manage this unprecedented situation, keeping purpose, conduct and wellbeing at the core of their actions.

The IA is committed to supporting members implement the operational resilience proposals as they come into effect. This is the second of our publications, following on from our work on defining important business services last year. This year, members can expect to see additional output, including guidance on setting impact tolerances in line with regulatory expectations.

For more information on how we support members please see our dedicated webpage: https://www.theia.org/operational-resilience

With the expected policy statements from the UK regulators on operational resilience in H1 2021, operational resilience is set to remain in the regulatory spotlight. However, as explored in this paper, it is clear effective governance of operational resilience is not just a compliance exercise, but instead holds great benefits for firms and good outcomes for the end investor.

We hope that this paper is useful to members as they continue their resilience journeys in 2021 and beyond.

EXECUTIVE SUMMARY

Focus on the operational resilience of investment firms and the wider financial sector has never been higher. Members recognise that achieving resilience to operational disruption is a strategic business imperative as well as a regulatory compliance area of focus.

Being resilient matters. Enabling consumers to meet their financial goals whilst meeting their obligations is crucial to maintaining trust through turbulent times. This is one of the reasons why it is a key concern for firms, their consumers, shareholders, regulators and the wider economy.

The IA, in collaboration with EY, convened member firms to discuss the importance of effective governance for operational resilience. Our aim was to distil key principles and guidance to help members shape their own approach. This paper sets out the following:

- Members' understanding of the key requirements
- Key principles for establishing effective governance of operational resilience and reporting
- Key challenges and potential steps to take
- Areas of focus and key questions for oversight and challenge of operational resilience governance

We believe that this paper will be useful because governance is an often nebulous topic. With operational resilience being a relatively new area of focus, it is easy to overcomplicate. There can be no one-size-fits-all solution. Whilst on the surface the topic can seem simple, operational resilience challenges us because it cuts across existing firm constructs and boundaries, and the threats organisations are constantly evolving. Some of these challenges are explored in **section 4**. Therefore, we are providing a set of principles and guidance to help members as they shape their own approach.

Our work with members highlighted that many are still in the early stages of their journey with operational resilience principles. This was particularly clear when focusing on effective MI and reporting. However, some messages were consistently considered important:

1. Members should adapt existing governance where possible to incorporate operational resilience oversight and decision-making.
2. Members should recognise the importance of the role of the board and senior management in directing, evaluating and monitoring the operational resilience framework.
3. Members should clarify strategic resilience aims and be consistent in the language that they use to talk about resilience internally and externally.
4. Members should not underestimate the importance of education and awareness throughout their organisations to build resilience thinking into their culture.

Five pillars of effective governance were identified in **Section 3**: **structures**, **roles and responsibilities**, **people and culture**, **enabling processes** and **subject matter**. Members' feedback on each of these themes are summarised alongside guidance on practical steps.

When reflecting on member feedback on how to get started, some 'no regrets' activities were identified:

1. Align leadership and senior stakeholders around strategic intent for operational resilience and agree on a mission statement or key principles.
2. Review the role of the board and key oversight mechanisms to ensure that the direction, evaluation and monitoring of operational resilience is in place, with processes to help role holders fulfil their accountabilities.
3. Consider roles and responsibilities across the three lines and for respective senior leaders to outline an initial governance model but recognise that it may need to be adapted over time.
4. Define training and awareness activities at all levels to consistently communicate 'what is resilience,' 'why it's important' and 'your role.'
5. Define operational resilience reporting using data that is available now, recognising that it will adapt as business services are mapped, impact tolerances are tested, and better data is produced.

A key component of effective governance is the evaluation of plans and monitoring of progress. We have provided key questions that those charged with oversight and assurance could consider in **section 5**.

2021 is going to be an important year for the industry. The sector has recognised the need to react to the evolution of regulatory expectations. Effective governance will be crucial in ensuring that performance is managed, risks to resilience addressed, and opportunities taken to achieve greater resilience firm-by-firm and across the market.

1. INTRODUCTION AND PURPOSE

Background and definitions

The Financial Conduct Authority (FCA) issued **Consultation Paper 19/32**[1] (CP) to help firms focus on the measures to reinforce their resilience. The CP is of most relevance to investment firms in scope for the 'enhanced' Senior Manager and Certification Regime (SM&CR), whilst the Prudential Regulation Authority (PRA) papers will also apply to those who are dual-regulated. Overall, there was little deviation in content from the initial 2018 Discussion Paper (DP), but rather the CP expanded and built on these concepts.

Within the CP, the FCA detail proposals for firms to communicate effectively in the event of a disruption. It covered existing governance requirements and their relevance to operational resilience, amongst other key priorities, such as identifying important business services and setting impact tolerances.

At present, there are a number of other factors driving firms towards more effective governance in respect of operational resilience. These include the outbreak of the COVID-19 pandemic, which forced firms to rethink their office-working strategy as well as a number of recent service outages within the financial services sector, the impending publication of the UK policy statements in early 2021 is also forcing firms' attention on more effective governance and operational resilience.

CP 19/32 indicates that, with respect to governance, firms should ensure that the board and senior management are clear on their responsibility and accountability, making certain they possess the relevant knowledge, experience and skills to adequately oversee and manage the requirements. There is an emphasis on the board using appropriate MI to inform investment decision-making around operational resilience.

The papers also include sections on outsourcing, recognising the implications of reliance on third-party suppliers and concentration risk. The UK regulators make clear that firms are responsible for governance of outsourcing and third-party relationships.

Dual-regulated firms may also be interested in the PRA's separate consultation on outsourcing, which details governance-related requirements regarding third- and fourth parties.

According to the Chartered Governance Institute, '*governance, the collection of rules, practices and processes by which an organisation is directed and controlled'* is foundational to improving the quality of decisions made by those who oversee businesses, enabling sustainable business models and creating long-term value'.[2]

Based on this definition, we will explore the different principles for governance, their interpretation and what this means for the IA member firms. Further to the FCA and PRA CP requirements, we will also leverage other global organisations' governance principles – such as Basel Committee on Banking Supervision (BCBS), The Board of the International Organisation of Securities Commissions (IOSCO), European Commission Digital Operational Resilience Act (DORA) and US Joint Authorities (the Federation) – comparing and showing direct alignment between global regulatory principles and the requirements set out above.

This paper will cover the differing regulatory and organisational considerations. It will examine the governance requirements for operational resilience that firms need to consider, and why. It will also address how to put the principles into practice, discussing how principle-based requirements translate into an effective governance framework with a focus on MI and reporting. Finally, this paper will explore the key challenges that firms are facing in establishing effective governance of operational resilience, and key areas of focus that those with individual and collective responsibility and accountability should consider.

IA activity

The IA's Operational Resilience Committee was formed to consider the proposals outlined in the DP. The committee has been supporting members with operational resilience through the consultation

[1] Source: 'Building operational resilience: impact tolerances for important business services and feedback to DP18/04' Consultation Paper CP19/32 December 2019, FCA (https://www.fca.org.uk/publication/consultation/cp19-32.pdf).

[2] Source: 'What is corporate governance', The Chartered Governance Institute, https://www.icsa.org.uk/about-us/policy/what-is-corporate-governance, accessed 29 October 2020.

process and will continue into the implementation period. This paper is being published as we await the publication of policy statements on operational resilience.

Understanding how to improve governance frameworks, particularly through the use of MI and reporting, is paramount to becoming more operationally resilient as a firm, as well as meeting evolving regulatory expectations. Improved governance frameworks also enable firms to streamline their priorities and take a more in-depth look at the dependencies on people, facilities, IT, data and outsourcers.

The IA convened the IA Operational Resilience Governance (Governance group) of more than 20 firms under the Operational Resilience Committee, throughout H2 2020. This group worked with EY to help investment management firms define their operational resilience governance structures and understand MI and reporting requirements. It was clear throughout the Governance group sessions that the member firms had a broad range of experiences and expectations with respect to governance, reporting and MI. This paper is the output of the Governance group, and is based on the synthesis of working group discussions and perspectives shared by members, as well as the experience EY has gained from working with firms to enhance their approach to resilience.

The summary of the output is shared with members and the wider industry to help build consensus on the steps needed to be taken to improve governance, MI and reporting, as firms look to enhance their operational resilience and comply with the policy statements. The guidance provided within this paper is, by its nature, generic for investment firms, hence each group will need to tailor it to their own needs and organisational structure.

The IA will continue to work closely with regulators through 2021 to represent investment management industry views through ongoing meetings and roundtable discussions, encouraging the regulators to adopt a proportionate supervisory approach.

2. REGULATORY AND ORGANISATIONAL CONSIDERATIONS

What are the governance requirements for operational resilience that firms need to consider, and why?

Firms' focus on governance is not solely based on achieving compliance with regulatory requirements – as set out in the FCA's[3] and PRA's[4] CPs – as better governance drives many benefits. Throughout 2020, many firms focussed their efforts on responding to the COVID-19 pandemic, with other activities de-prioritised. When the Governance group convened in H2 2020, the combined effect of stabilisation of the pandemic response and the anticipated publication of policy statements shifted many firms' focus towards the importance of good governance.

Benefits of an effective governance model for operational resilience:

Whilst member firms recognise that they are obliged to meet regulatory requirements with respect to operational resilience, they also see the business benefits. Based on discussions with members in the Governance group, and the experience EY has gained in the industry, we collectively identified the following benefits:

- **Clarity of organisational direction, roles and responsibilities:** firms are able to streamline their priorities across the organisation, working cohesively to enhance resilience when a strategic direction is set through effective governance.
- **Visibility of performance and risk to key decision-makers:** firms are able to work with an added degree of transparency, enabling effective evaluation and monitoring of resilience performance and key risks.
- **Better coordination across silos:** firms bring together teams across business and technology to work towards achieving goals and reaching better resilience outcomes.
- **Reduced duplication and inefficiency:** firms foster a culture of teaming across the business, without reproducing work within different business areas or teams.
- **Enabling individuals and boards to discharge their accountabilities:** firms have the right structures and support mechanisms in place to enable individual and collective accountabilities to be met, and robust evidence maintained to demonstrate that reasonable steps have been taken.

Summary of key international regulatory expectations:

Whilst Governance group workshops were being held during H2 2020, there were several significant additions to the global regulatory landscape which complement the FCA and PRA CPs:

- **International Organization of Securities Commissions (IOSCO)** principles on outsourcing[5] (May 2020)
- **Basel Committee for Banking Standards (BCBS)** CP on principles for operational resilience[6] (August 2020)
- **European Commission** Digital Operational Resilience Act (DORA)[7] (September 2020)

[3] Source: 'Building operational resilience: impact tolerances for important business services and feedback to DP18/04' Consultation Paper CP19/32 December 2019, FCA (https://www.fca.org.uk/publication/consultation/cp19-32.pdf).
[4] Source: 'Operational resilience: impact tolerances for important business services' Consultation Paper CP29/19 December 2019, PRA (https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf).
[5] IOSCO sets out seven key expectations for regulated entities that outsource functions, processes and systems. The paper highlights governance as a key area for consideration when selecting a potential third-party service provider. These principles are based on a joint project between the IOSCO board and committees, including secondary markets, regulation of financial intermediaries, and credit-rating agencies and derivatives, with the aim of assessing whether the existing principles for outsourcing remained suitable, and whether any updates were necessary. For further information see 'Principles on Outsourcing' Consultation Report CR01/2020, IOSCO (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf).
[6] BCBS sets out seven key principles for operational resilience. Typically adopted by global regulators, their approach is noteworthy. However, this paper is not directly applicable to the majority of the IA's members. For further information see 'Principles for operational resilience' Consultative document, BCBS (https://www.bis.org/bcbs/publ/d509.htm).
[7] The European Commission initiative proposes six areas in which digital operational resilience can be achieved, through oversight, testing and risk management procedures of information communication technology (ICT) risks and incidents. This proposed act is specifically focused on IT and IT supplier resilience, and will not be in force for several years. However, it demonstrates the European regulatory direction of travel with respect to resilience. For further information see 'Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector', European Commission (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595).

- **US Joint Authorities'** paper on operational resilience[8] (October 2020)

These emerging regulatory requirements complement the existing requirements that member firms are already subject to, such as the FCA's Principles, Systems and Controls as well as the explicit principles defined in the UK CPs.

Application of the SM&CR and role of Senior Managers

The FCA paper identifies the Senior Manager Function (SMF) 24 (Chief Operations Function)[9] as the executive with accountability for the firm-wide approach for achieving operational resilience. This function Is only a requirement for firms operating under the Enhanced SM&CR regime, which reflects the formal scope of the resilience regulations.

Through discussion, many members agreed that firms without a formally designated SMF24 were appointing responsibility to operations and technology executives who would reasonably be expected to be the SMF24 if the firm were to be subject to the regime. Firms are also considering the importance of the role of the SMF 4 (Chief Risk) given the relationship between risk management and resilience. Many international firms are also considering the increased emphasis in emerging US and Basel Committee papers on the role of the second line in an effective resilience management system.

From reviewing the requirements in the sources identified above, the following expectations were identified and aggregated across five key themes:

- **Structures:** key components including committees, reporting lines, role of the three lines and establishment of governance bodies and their mandates.
- **Roles and responsibilities:** key individual and collective roles from the board and executives down.
- **People and culture:** the strategy, principles and cultural elements that operationalise good governance.
- **Enabling processes:** key activities within a member firm that enable good governance, such as policies, procedures and MI generation.
- **Subject matter:** key topics and areas of focus that should be directed, evaluated and monitored.

[8] The US Joint Authorities' paper details seven key sound practices to be enforced to achieve operational resilience. This paper is applicable for larger global IA member firms and major service provider groups such as custody banks and fund administrators. These sound practices are heavily based on the BCBS principles and are the first public adoption by a major regulator. For further information see 'Sound Practices to Strengthen Operational Resilience', Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency joint paper (https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf).

[9] FCA 19/32 defines SMF24 – Chief Operations Function – as 'the most senior person responsible for managing the internal operations (including HR), systems and technology of a firm'. Source: page 27 of 'Building operational resilience: impact tolerances for important business services and feedback to DP18/04' Consultation Paper CP19/32 December 2019, FCA (https://www.fca.org.uk/publication/consultation/cp19-32.pdf).

3. PRINCIPLES INTO PRACTICE

3.1 How do these principle-based requirements translate into an effective governance framework?

Based on analysis above, the following key components of an effective governance framework were identified:

Whilst it will be up to each firm to determine precisely how they achieve good governance for operational resilience, key practices that were discussed with members are set out below. Practical examples, where identified, are included to support members in deciding their own approaches.

Structures

Structures, such as committees, reporting lines, mandates and terms of references, are the basis upon which effective governance is built. Member firms highlighted the importance of aligning to the BCBS operational resilience CP principle of reusing or adapting existing governance, where possible. Taking this principle into account, the following areas of focus were identified:

Committees and reporting lines	
Principle: Firms should adapt existing governance structures to establish, oversee and implement an effective operational resilience framework.	
Member perspectives: Members reported a range of approaches regarding the use and role of existing executive committees with respect to operational resilience as part of their governance framework. Most members embraced the BCBS principle of adapting existing governance structures to incorporate operational resilience rather than creating new reporting lines or committees in the early stages. Some reflected that this might be required	**Practical steps to take:** Given this context, the following steps were put forward for consideration: • Establish working or steering groups focussed on embedding new operational resilience requirements. These typically bring together business, operations, technology, cyber, supply chain, risk, compliance and audit stakeholders. • Review board reporting lines, and consider the topic being reported to either the full board or delegating responsibility to the board risk committee to be the ultimate oversight committee.

at lower levels, for example to review groups of important business services and thematic findings across technology or the supply chain, but that this would be future state rather than part of implementation. Many firms noted that existing resilience committees had been repurposed to respond to the early stages of the COVID-19 pandemic crisis, but in H2 2020 reverted to focusing on broader operational resilience requirements. Firms noted an uptick in board interest and awareness of operational resilience, and hence had adjusted agendas or added special sessions as short-term approaches to inform the board whilst management considered next steps.	• Align executive reporting lines to the ultimate board reporting lines, whether these are operations committees or risk committees respectively. • Identify opportunities to simplify existing reporting lines on capabilities that support operational resilience to bring together discussion on important business services and the key preventative, response, recovery and communicative capabilities within one forum. • Review opportunities to embed operational resilience performance and risk management topics into existing governance committees, for example reporting on technology gaps and issues in existing technology oversight forums.

Role of the three lines

Principle: Firms should consider the roles of business management, an independent risk function and independent assurance functions as part of the operational resilience governance framework.

Member perspectives:	**Practical steps to take:**
The roles of the three lines in their operational resilience work varied amongst members. Firms recognised the emphasis on the role of first-line business, technology and operations in owning the operational resilience outcomes through business-as-usual, as well as during the pandemic. However, increasing emphasis from global regulators on the role of risk professionals has confirmed the importance of the role of the second line as part of an effective governance structure. Firms welcomed the FCA's stipulation in their CP that the SM&CR is designed to be applied flexibly to accommodate different business models and governance structures.	During working sessions, three options were explored and are shared for consideration by firms: • A second-line risk-led model where the focus is on the role of the second line to define an operational resilience framework for the first line to implement. • A first-line business- or operations-led model with the framework and approach definition being led within the line of business or operations teams. The role of the second line typically overseeing and challenging the framework set out by the first line as well as getting more involved in testing and quality assurance activities. • A mid-way 'one-and-a-half' line team taking the lead on operational resilience and defining the framework, which is then provided to business lines to implement with support and guidance from the central oversight team. In this model the role of the second line is typically to oversee and challenge the framework and execution within it.

Mandate, membership and terms of reference

Principle: Firms should ensure that stakeholders from across the three lines are involved in operational resilience governance, and that individual and collective mandates are clearly defined, documented and reviewed for effectiveness.

Member perspectives:
Many members commented that their committees, reporting lines, roles and responsibilities were in the early stages of forming, or that they were assessing changes that may be needed to existing structures to adapt to holistic operational resilience requirements.

Many had not yet re-visited their committee mandates or terms of reference to include operational resilience explicitly but noted that key capabilities required to manage, and monitor resilience were part of existing structures.

Practical steps to take:
Given this context, the following steps were put forward for consideration:

- Document the mandate of committees (including any delegations) throughout the end-to-end governance structure with respect to holistic operational resilience, considering changes identified in *committees and reporting lines* above.
- Review membership of committees to ensure that the breadth of disciplines required to contribute to the agenda are represented from across the three lines. Note the emphasis on resilience being business-led and consider the role of senior leaders responsible for business service provision in committee membership.
- Consider the lessons learned from the pandemic response, particularly focusing on the clarity and decisiveness of decision-making as well as the identification of additional participants with roles to play in maintaining resilience through the crisis.
- Revisit the mandate, membership and terms of references periodically.

Roles and responsibilities

Defining clear roles and responsibilities for the board and senior management helps to ensure firms meet key individual and collective role requirements, maximising efficiency, improving decision-making, and ultimately enhancing the firm's operational resilience. Members offered examples of their varying governance arrangements for operational resilience. Members agreed during working sessions that the UK authorities have made it clear that the board and senior management have ultimate oversight of the resilience strategy and are responsible for promoting a resilience culture, both of which are principles echoed in the BCBS papers. Taking this principle into account, the following areas of focus were identified:

Role of the board

Principle: The board should be able to demonstrate that it is responsible for directing, evaluating and monitoring the operational resilience framework and is able to make informed resilience-related decisions.

Member perspectives:
Members reported mixed experiences with the roles of their boards, board risk committee or equivalents at present regarding operational resilience, including:

- Consideration of varying the responsibilities of operational resilience between the full board and delegation to the risk committees of the board, depending on the existing agendas, responsibilities and

Practical steps to take:
Given this context, the following steps were put forward for consideration:

- The board or committees of the board (such as the Risk Committee) could provide input on the strategic intent and high-level appetite for operational disruption to demonstrate that they direct the resilience agenda.
- Document the role of the board and any delegations to committees of the board for the direction, evaluation and monitoring of operational resilience.

preferences of the chairpersons and governance officers.

- Agreeing that their boards had been engaged with resilience throughout the COVID-19 crisis; however, also noting regulatory soundings that a strong response to the pandemic does not mean a firm is 'resilient enough' in all severe but plausible scenarios. This message was considered important to set expectations for the work required through 2021 and beyond.

- Hold training and awareness sessions with boards on regulatory expectations and put forward perspectives on what this might mean regarding the board's roles and responsibilities for evaluating management's plans and monitoring updates on progress.

- Ensure that boards have access to relevant expertise to inform their decision-making, with some considering the appointment of independent non-executive directors with operations and technology experience or setting up direct channels to independent advisors to support the board in evaluation and monitoring activities.

- Consider the requirement for the operational resilience 'self-assessment' to be reviewed by the board, and hence document the reporting lines and awareness exercises required to enable effective engagement with the board on this exercise.

Senior management

Principle: Senior management (including relevant Senior Managers) should be able to demonstrate clear accountability for the firm's operational resilience framework, with delegations and shared responsibility being well-articulated. Role-holders should have sufficient authority, expertise, resources and access to the board to execute their roles.

Member perspectives:
Not all members of the Governance group are required to designate an SMF24, which includes accountability for operational resilience. Smaller firms recognised the principle that resilience requires inputs from across the business, operations and technology, with senior executives in equivalent roles having significant inputs to the operational resilience agenda.

Members noted that during the COVID-19 pandemic, many senior business, operations and technology stakeholders had been convened either as part of crisis groups or longer-term pandemic Governance groups. Some firms repurposed their operational resilience steering groups to oversee the pandemic response. Many recognised the lessons learned from the pandemic, including the pace of decision-making that could be achieved when required.

Members reported different approaches to allocating the SMF24 role should they have one, with some splitting the role between operations and IT leaders through documented statements of responsibilities. Some firms also highlighted the importance

Practical steps to take:
Given this context, the following steps were put forward for consideration:

- Defining the governance structures around SMF24s or equivalents to support them in demonstrating oversight and engagement with operational resilience.

- Establish operational resilience steering groups, which would in time be chaired by the SMF24 or equivalents, with the steering group supported in larger firms by working groups focused on delivering aspects of the resilience framework. Where there is heavy involvement of the risk function in setting the direction, the SMF4 could have a formal role in co-chairing oversight or steering committees.

- Recognise the importance of engagement with senior business leads who would ultimately have a role 'owning' a business service.

- Expect healthy tension between business leads (who may be designated SMFs in their own roles such as SMF6 (Head of Key Business Area) in larger firms) and SMF24s who are typically responsible for supporting people, processes, technology, suppliers, facilities and data enabling business services to be delivered.

- Define roles for senior business leaders involving day-to-day oversight, ownership and direction of important business services. Key roles could be defined for maintaining key components of the services framework, such as service mapping, impact tolerances and scenario testing, which could be split across the first and second line depending on a firm's approach to defining the framework.

of the role of the SMF4 in integrating resilience outcomes into the risk management framework and overseeing activities in the first line.	• Review the authority, training, potential for conflicts of interest, access to resources and reporting lines supporting key role-holders. Consider potential blockers that need to be addressed to avoid roles being (or being considered) paper exercises.

People and culture

Effective governance is underpinned by the people driving resilience initiatives and the fostered culture within firms. Members recognised the need to align their organisations around a common purpose and the understanding of operational resilience, but few had made material progress.

Strategy, appetite and principles

Principle: The firm should clearly articulate its operational resilience objectives and appetite for disruption, as well as how it intends to operate within them.

Member perspectives: Some members reported a need to clarify the firm's strategies and principles for operational resilience. Whilst regulatory drivers were front of mind for many, some identified wider business benefits for their organisation of better aligning resilience and risk management activities to business services and consumer outcomes.	**Practical steps to take:** Given this context, the following steps were put forward for consideration: • Align leadership and senior stakeholders around strategic intent for operational resilience and agree on a mission statement or key principles. • Bring this intent to life through consistent communications from senior leaders on the importance of resilience and key principles of the firm's approach. • Review risk appetite statements relating to disruption to consumers, markets and the firm's safety and soundness and consider setting a broader appetite for operational disruption. Cascade this firm-wide appetite through discussions on important business services, impact tolerances and testing to compare what the firm wants to achieve (appetite) with what the firm must achieve (impact tolerance) in a range of scenarios. • Refresh the stated ambition, appetite and intent on a periodic basis as the firm's resilience approach matures, and as organisational priorities change to ensure that they remain relevant. • Identify opportunities to align resilience principles with business drivers and strategic initiatives. An example of this might be infusing resilience and quality of service even during disruptions into strategic programmes around digital consumer journeys or re-platforming.

Culture, skills and expertise

Principle: The firm should focus a strong level of awareness of and commitment to operational resilience, recognising that staff at all levels have important roles to play. Key role holders across the three lines maintain appropriate skills and knowledge to understand and manage risks to operational resilience and keep them current.

Member perspectives: Members recognised the importance of culture to embed operational resilience	**Practical steps to take:** Given this context, the following steps were put forward for consideration:

principles and activities into day-to-day operations. Members reported the need for relevant knowledge, skills and expertise across the board, the senior management and the entire firm. *Note that board composition, awareness of resilience within the senior management and training needs are the areas explored above.*	*Culture:* • Translate strategy and principles to meaningful behaviours and measurable outcomes that can be integrated into the roles and responsibilities of individuals across the organisation. • Define training and awareness activities at all levels to consistently communicate on 'what is operational resilience,' 'why is it important' and 'what is your role.' • Consider the importance of 'tone from the top' - from the board and senior management during the rollout of new activities as well as during and after an operational disruption or crisis. • Emphasise the importance of prevention, response, recovery, learning and communication as key components of being resilient. *Skills:* • Review the blend of skills for the team defining and overseeing the operational resilience framework taking into account the need for resilience teams to both manage change across the firm through good communication and engage in detailed data analysis to assess resilience capabilities and gaps. • Identify opportunities to better engage business-line risk and control teams in operational resilience activities to combine their knowledge of business services with the operational framework and tooling. • Review the approach to assessing the skills and knowledge of key staff across the three lines to ensure that requisite experience is in place to plan, oversee and challenge resilience initiatives.

Enabling processes

Effective governance cannot be achieved in a vacuum, and members identified certain key activities that are crucial to supporting direction, evaluation and monitoring of operational resilience outcomes.

Reporting structures

Principle: The board and senior management should be able to place reliance on reporting structures for the governance of operational resilience to support their views and decision-making.

Member perspectives: Members recognised the need for day-to-day reporting structures to support the more periodic executive committee structures highlighted above.	**Practical steps to take:** Given this context, the following steps were put forward for consideration: • Adapt existing technology, third-party oversight, data, facilities and HR forums to consider operational resilience considerations for the resources supporting important business services. • Identify opportunities to bring together business service owners (if defined) to review thematic challenges and strategic investment decisions for resilience on a regular basis.

Taxonomy

Principle: A firm should clearly define the language used to talk about resilience to ensure that communication, reporting and decision-making on the topic is using consistent and well-understood terminology.

Member perspectives:
Members commented on the need to streamline the language used across the firm to minimise confusion, align reporting, enable repurposing of knowledge and information, and ultimately avoid inefficiencies and inconsistencies.

Practical steps to take:
Given this context, the following steps were put forward for consideration:

- Agree and document key terminology used within the firm's resilience framework such as 'important business services' and 'processes'.
- Review potential overlaps with language used elsewhere in the organisation such as terminology used within the wider risk framework.
- Engage with critical third parties and providers to compare resilience terminology used within key documentation and reporting to ensure alignment where relevant.

MI and reporting

Principle: There should be a meaningful, end-to-end flow of information on resilience related matters within the firm which enable effective direction, evaluation and monitoring of operational resilience outcomes.

Discussions with members, specifically on reporting requirements for operational resilience, are captured as part of **section 3.2** below.

Policies and procedures

Principle: Key components of the resilience framework including governance and oversight requirements, ownership and accountability, key principles and approaches to achieving them should be documented.

Member perspectives:
Whilst members did not consider documenting policies and procedures to be a cure-all for resilience challenges, many were considering documenting the key requirements.

Members noted that it may not be efficient to create new policies and handbooks specifically for operational resilience but were looking at adapting existing documentation to include key concepts like business services and impact tolerances. Some saw the opportunity to refresh their policy framework for key capabilities enabling resilience (such as business continuity and crisis management) but this was not an immediate priority.

Practical steps to take:
Given this context, the following steps were put forward for consideration:

- Document key requirements in a policy or integrating operational resilience concepts into existing policies. Members were divided in their approach and were typically led by their existing organisational approach to policies and frameworks.
- Document key procedural steps associated with identifying important business services, mapping them, setting impact tolerances, carrying out scenario testing and prioritising investments.
- One area that members may also wish to consider is the integration of operational resilience concepts into other existing protective disciplines, such as information security, business continuity and IT service management.

Assurance across the three lines

Principle: The governance framework for operational resilience (including MI and enabling processes) should be continually assessed for effectiveness.

Member perspectives:
Members highlighted varied approaches to the roles of the three lines in their operational resilience work at present.

Many firms highlighted that their internal audit functions had started to review their approach to achieving compliance with the CP principles whilst also continuing to review key components such as business continuity as part of their audit plans.

Practical steps to take:
Given this context, the following steps were put forward for consideration:

- Define explicit roles for the second and third line in the operational resilience programme (if defined) and business-as-usual resilience management.
- Review assurance activities (i.e. controls testing, thematic reviews, audits) conducted across the three lines holistically to identify gaps or inefficiencies.
- Revisit how assurance activities are reported on to senior management and the board to present a consolidated view on operational resilience.
- Emphasise the role of the second and third line in assurance and challenge over MI and reporting considering quality, coverage and lineage.

Subject matter

Subject matter

Principle: The firm's governance framework should consider information on the breadth of functions and processes that enable resilient outcomes. Key role-holders should be able to demonstrate decisions, oversight and monitoring of operational resilience outcomes.

Operational resilience is, by definition, an outcome that is contributed to by numerous existing capabilities and functions. The challenge that many members face is prioritising information to feed through governance and reporting structures. **Section 5** of this paper considers key questions and focus areas that could be used to help structure point in time and regular reporting on operational resilience.

3.2 How does MI and reporting support effective governance and how are member firms approaching this?

Discussions with members as part of the Governance group identified that operational resilience as an outcome, is in many ways, harder to measure than financial risk and resilience. Some member firms were at early, conceptual stages in defining their business services but were keen to think ahead to the key principles of reporting so that information was captured as part of the process.

Working sessions on MI and reporting primarily focused on two areas:

- The current state of operational resilience MI and reporting
- Members' reflections on the future state for reporting and how it might support the governance principles set out above

Members agreed that this topic would require revisiting through 2021 as more information and data were available, and as governance bodies matured and requested more or different MI and reporting. In the meantime, some practical next steps are suggested to help members as they define their own MI and reporting.

Summary of the current state of MI and reporting for operational resilience:

Members agreed that multiple sets of MI and reporting are currently being generated on capabilities that make a firm 'resilient'. The areas highlighted by members are broadly aligned to the key capabilities identified by the BCBS principles for operational resilience, as set out in the diagram below:

It was broadly agreed by members that these metrics, whilst often reported in different places and at different times, already generated good debates and discussion, even if they are not focussed on important business services.

Some limitations identified by firms with respect to the currents state of reporting and MI included:

- Much of the current reporting on operational resilience principles are focused on the impact of the regulation and high-level plans for programmes.
- Current risk data, MI, reporting and actions for resilience are captured and tracked, but are not considered specifically through the business service lens as foreseen in the UK CPs. Many risk management systems are not configured for the demands of operational resilience.
- Existing risk appetite statements and metrics are typically focused on the impact to, or losses for, the firm, rather than disruption to consumers and the market.

The challenge identified was that the aggregation, analysis and reporting of these metrics and data would need to be adapted in order to fulfil the needs of those absorbing it for the purpose of operational resilience oversight, governance and compliance management. Members agreed that MI needs to clearly highlight the actual and predicted performance against the stated impact tolerances for each important business service and be aggregated into a firm-wide view on the position against tolerance for disruption.

Members' reflections on the future of MI and reporting for operational resilience:

Members considered a conceptual model of information and reporting flowing throughout a generic 'firm' and agreed that it would be pragmatic to design new principles for MI and reporting based on the structure of the governance framework.

The conceptual model focussed on three 'tiers' of reporting, namely:

Board-level reporting	
Purpose: Strategically focussed and enabling effective direction, evaluation of management decisions and monitoring of outcomes.	**Principles to consider in MI and reporting:** • Review, challenge and approval of the firm's resilience strategy and framework. • Periodic updates on the progress of an operational resilience programme to implement UK CP requirements, including identification of important business services, setting of impact tolerances, and progress and outcomes of scenario testing, including senior management rationale for key decisions made through this process. • Provision of analysis and commentary on key threats and vulnerabilities and trends as well as emerging trends with respect to important business service resilience. • Outcomes of significant testing as well as material internal and external incidents. • Plans for major investment decisions, and highlights of how resilience is considered within them or driving them. • Mandatory review, challenge and approval of annual self-assessment documentation.

Senior management-level reporting	
Purpose: Balancing detailed examples with thematic insights to support timely decision-making and change management throughout the firm and supporting SMF holders or equivalents with oversight and decision-making with respect to operational resilience.	**Principles to consider in MI and reporting:** • Review and recommend for approval by the board of strategy and framework. • Regular updates on the operational resilience programme, including lessons learned from stakeholders involved, such as business service owners; and ratification of key decisions made throughout the programme. • Reporting aligned to important business services (to enable drill-down) as well as aggregated reporting for key themes. • Review of firm-wide and more specific risks, key trends, emerging threats to resilience considering the firm's ability to prevent, adapt, respond, recover, learn and communicate. • Review of results from business services framework (identify, map, set tolerances, test and remediate) as well as oversight of key capabilities such as business continuity and incident management.

Day-to-day management-level reporting	
Purpose: Oversight and monitoring of business services, technology, operations and key capabilities supporting operational resilience; and regular engagement on key successes, key risks, vulnerabilities and decisions to be made.	**Principles to consider in MI and reporting:** • Initial approval of business services framework artefacts, such as identification of important business services, setting impact tolerances and results of scenario testing. • Review of resilience trends and vulnerabilities as well as changes to the risk profile of important business services through monitoring of key performance indicators (KPIs) and key risk indicators (KRIs) linked to business services, for example, failed changes or breaches of service level agreements (SLAs) for resources supporting an important business service, allowing more precise monitoring of the impact on consumer outcomes. • Asset level review of technology resilience, facilities resilience, people and process resilience, data, and supplier resilience metrics, ideally with asset level metrics measuring performance and risk relating to important business services. • Review of key capabilities, such as business continuity, incident management, IT disaster recovery and crisis communications with respect to important business services. • Consideration of the outcomes of assessments and testing to prioritise risks, gaps, investments or risk acceptances.

Challenges identified

Members identified several challenges and blockers to enhancing MI and reporting as firms progress with a model such as this in the future:

- Several **technology constraints**, including the timeliness of data, came to light. Members recognised the need for a range of reporting focussing on both point-in-time reporting for governance bodies reviewing the previous period and making decisions, versus real-time data needs during an incident. The complexity of pulling together multiple existing sources of data (such as a Configuration Management Database (CMDB)) and aligning them through the business service lens was recognised as a key blocker without significant effort.
- There were **differing definitions** of terms, such as 'important business service,' across regulatory jurisdictions and differences in the understanding of key terminology across firms at present. Hence, focus is placed on 'taxonomy' in **section 3.1** above.
- The current lack of clarity regarding the frequency of **MI and reporting requirements** resulted in members recognising the need for an annual self-assessment and anticipating the need for senior management and boards to review key reporting more often. Agreeing to the cadence for programme updates was an area of focus for multiple members at the point of the working sessions.
- The **cultural shift** away from functions reporting in silos towards a wider information sharing chain focussed on business services.
- Identifying changes, such as a **new service or product** being implemented, and diagnosing the impact on operational resilience or on the management of business services is another challenge. Countering this challenge will enable better identification of triggers, such as incidents and changes.

Practical next steps

Practical steps that members considered through the working session included:

1. **Define tactical reporting** using data that is available to give a perspective on the firm's resilience, recognising that metrics aligned to business service resilience may not be developed yet but may be useful for communication and change management if there is disciplined, consistent reporting.
2. **Build resilience reporting into pilots** of important business services to demonstrate the 'so what' from identification, mapping, tolerance setting, testing and remediation planning activities.
3. **Outline a framework** for reporting and MI which defines the key questions to be answered in reporting and the level of granularity to be aimed for at different levels – such as board, senior management and day-to-day management levels.
4. **Engage with boards, senior management and key role-holders** to gather business requirements for future-state reporting on resilience. Key questions that might be considered in this reporting are set out in **section 5** below.
5. **Explore adoption of tooling** to support the rollout of their important business services approach or adapting to existing tooling where possible. As part of this, focus was highlighted on the data model required to feed regular reporting on operational resilience, including the identification of golden sources of data outside the ownership of a resilience team or programme.

4. PRACTICAL CHALLENGES

What are the key challenges firms face in establishing effective governance of operational resilience?

Members identified a range of issues that could be caused by ineffective governance of operational resilience. Ineffective governance might mean weaknesses in the direction setting for operational resilience, the evaluation and challenge of management's plans, or poor monitoring of progress against plans. Potential issues include:

- Incomplete or inaccurate alignment of operational resilience to the UK regulatory requirements. Missing explicit regulatory expectations may lead to steps being taken against the firm and individuals with specific accountabilities.
- Inefficient adoption of operational resilience approaches, leading to overwork, rework and loss of support for initiatives, which might include poorly informed or unchallenged investment decision-making.
- Lack of support for the operational resilience from one or more functions, leading to limited progress
- Design decisions being made that might reduce the firm's ability to change in the future.
- Limited understanding of engaging and managing risks to resilience, which could harm consumers and the firm itself.

Specific challenges beyond those outlined throughout **sections 3.1** and **3.2** that members identified in their work to date regarding operational resilience and governance included:

Global vs local requirements

For large multinational firms, local operational resilience governance requirements may not align with the demands of global regulators. Careful consideration must be taken to ensure that the firm not only remains complaint across all jurisdictional areas but that it remains efficient and avoids duplication of efforts.

Members noted that for global firms, it is useful to have a common global operating model and draw out common themes relating to resilience, but this may not be simple depending on the future of regulatory developments.

Members with a global footprint highlighted that it could be difficult to integrate the UK's senior manager framework if you are a global firm with senior roles that are based outside the UK. In answer to this, it was suggested that whilst you could assign an SMF position outside the UK, this may raise challenges from regulators. As a result, effective governance structures to support such an individual in demonstrating their execution of accountabilities is important.

Third-party oversight

Many member firms are heavily reliant upon third parties in maintaining their business services, with key functionality and infrastructure held off-site. Some of these relationships are driven by consumer choice rather than firms' own selection criteria which might include resilience, for example when clients select a custodian. Wherever service provision is supported by an external party it is imperative that firms maintain oversight of these third parties with appropriate risk data to build an accurate view of their risk and resilience portfolio.

There were mixed experiences amongst members who had started to engage with critical third parties on operational resilience. Many service providers, who generally are not directly regulated, are not well advanced on the topic. However, some are bringing groups of regulated clients together to proactively engage in operational resilience, which is seen as a positive step for the industry. The availability of quality, specific data and reporting on resilience from third parties was also a common challenge amongst member firms and considered a limiting factor in firms' own MI.

Data and reporting

Resilience is a dynamic concept and requires a mindset of continuous monitoring and improvement. For many firms, their current MI capabilities will include all the required information to consider resilience holistically as a firm. However, the challenge is in taking the right cut of the data and aligning it to business services to bring generic risks and vulnerabilities to life through potential impact on consumer outcomes.

Section 3.2 explores challenges and opportunities relating to MI and reporting in more detail above.

Self-assessment

The expectations for a self-assessment document, that would be made available to the UK regulators following implementation of the principles as set out in the December 2019 CPs, remain unclear. We expect further clarity in the policy statement.

One consideration for members is that, depending on typical lead times for their governance bodies, the requirement for a self-assessment to have been approved by the board by the end of the implementation period may reduce up to two months' time from firms' 'plan for compliance'.

5. AREAS OF FOCUS

Once governance is established, what are the key areas that those with individual and collective responsibility should be considering?

Each member firm's own board and senior management will have their own priorities based on organisational strategy, consumer or client base, and known vulnerabilities. Members taking part in the Governance group agreed that there should not be recommended areas of focus or agendas, given the principle that firms should adapt this guidance to their own context and agendas. However, the following example key questions are provided to aid:

1. Non-executive directors, senior managers and those in risk and audit functions to support with oversight and challenge of operational resilience areas of focus.

2. Those charged with establishing operational resilience frameworks within member firms to assess their own position against these questions and address any issues identified in a timely manner.

Potential challenges raised by member firms and experience that EY has gained in the industry have been set out below, with example practical steps that might be taken to address them.

Key question	Potential challenges	Potential ways to address challenges
Does the board have the relevant **skills and experience** to know if we're doing enough?	• The evolving technology and outsourcing landscape bringing new and changing risks • Limited experience across the industry as firms adapt to regulatory and good practice guidance • Lack of the right skills and experience limiting the effectiveness of independent direction, evaluation and monitoring of key nonfinancial risk and resilience areas	• Area review the current composition and skills within the board • Conduct training as necessary to bridge the gap • Consider appointing skilled independent advisors to supplement skills and experience on the board
Do our Risk Committee, Audit Committee and board **sufficiently debate** the resilience of the organisation and **understand** their remit and delegations?	• Embedding and prioritising operational resilience within existing regular governance discussions or establishing new forums • Discussions about 'resilience' focus overwhelmingly on recovery capabilities and backwards-looking measures	• Ensure that committee terms of reference and attendees represent business, operations and protective disciplines (e.g. business continuity and crisis management) focused on operational resilience • Clarify terminology used in reporting across three lines with respect to resilience • Consider both forward-looking and historical metrics when designing MI and reporting • Refine the scope of the resilience framework to ensure balance between prevention, detection, response and recovery capabilities
Do we have an operational resilience strategy that covers **people, processes** and **technology** and our significant third- and fourth-party dependencies?	• Lack of defined strategy that is aligned to regulatory expectations, including a robust implementation programme plan • Gaps in coverage of key resources or capabilities that support operational resilience, or overwhelming focus on one area (such as business continuity, or third party oversight)	• Write a high-level operational resilience strategy that sets out the firm's approach to business services and links to key resources (i.e. people, technology, data, facilities, third parties) and existing protective disciplines (e.g. continuity, recovery, crisis management) • Review current resilience capabilities against regulatory expectations and industry-leading practices to baseline current state

Do we understand our **'crown jewels'-** the important business services we provide that matter most to our consumers and the wider market?	• Focus of operational resilience activities being inefficient or ineffectively directed • Communication of priorities and focus areas being overly technical and not linked explicitly to business priorities and outcomes	• Define a taxonomy of business services that the firm provides, then use repeatable criteria to determine which are 'important' based on four regulatory drivers (consumer, market integrity, firm impact and financial stability) • Consider services which are 'important' to the firm, but not the regulatory-driven assessment and 'internal' services identified as common dependencies through the second phase of a programme
What are the '**severe but plausible'** disruption scenarios that our organisation is preparing for?	• Focus being placed on previous incidents or crises, rather than considering the wider range of events that could cause operational disruption • Scenarios defined not severe or plausible enough to stress firms' ability to remain within impact tolerances	• Define a library of scenarios and the 'levers' that can be pulled to make them more or less severe - this may build on existing operational risk scenarios but will likely be more extensive • Validate this list of scenarios with key stakeholders across the three lines • Develop a testing approach from which the result can be evidenced in terms of actions taken and decisions made
What are the **key vulnerabilities** (gaps in our resilience capabilities) that we need to focus on the most?	• Reporting on resilience being overly focused on 'good news' and not highlighting key areas of focus to enhance resilience • Reporting on vulnerabilities not linking to important business services and user outcomes, and therefore seems theoretical	• Define reporting that highlights key vulnerabilities, making this thematic at higher levels across the organisation • Use examples of how vulnerabilities might affect resilience of business services and their ability to remain within impact tolerances to support reporting and 'make it real'

APPENDIX

Outline summary of regulatory guidance and expectations

The summarised requirements and principles outlined below are provided as an indicative guide and should not be relied upon as an exhaustive list. Many of the source documents (see footnotes in **section 2**) are consultation or draft documents at the point of reporting, hence should be reviewed in context for the most up to date.

Key Theme	Key points	Requirement or principle	Informative reference
Structures: key components including committees, reporting lines, role of the three lines and establishment of governance bodies and their mandates	Firms should utilise their existing governance structure to establish, oversee and implement an effective operational resilience approach.	Consultation principle	BCBS Principle 1[10] DORA Chapter II – ICT Risk Management, Section I, Article 4[11]
	Firms should align to existing senior management arrangements, systems and controls.	Requirement	FCA – Chapter 7 PRA – Chapter 4 FCA – SM&CR
Roles and responsibilities: key individual and collective roles from the board and executives down	Firms should ensure board and senior management have enough time to establish business and risk strategies relevant to operational resilience and culture.	Consultation requirement	FCA – Chapter 7 PRA – Chapter 4
	Boards should review and approve resilience expectations, risk appetite and tolerance for disruption.	Consultation requirement	BCBS Principle 1 US Joint Authorities' paper 1(a)[12]
	Boards should actively communicate firm's approach to operational resilience.	Principle	BCBS Principle 1
	Firms should implement specific accountabilities under the SM&CR (e.g. SMF24 or equivalent) for operational continuity, resilience and strategy and may find that the responsibility for operational resilience proposals under the operational resilience CP falls within scope of the SMF24's responsibilities	Consultation requirement	FCA – SM&CR FCA – Chapter 7
	Senior management is accountable for maintaining a detailed, accurate and regularly updated overview of the firm's organisational and legal structure that identifies the critical operations and core business lines of the firm and its material entities.	Consultation requirement	US Joint Authorities' paper 1(b)
	Firms' management body will be required to maintain a crucial, active role in steering the ICT risk management framework and shall pursue the respect of a strict cyber hygiene.	Consultation requirement	DORA Chapter II – ICT Risk Management, Section I, Article 4
	Firms' management body's responsibility in managing their ICT risk includes the assignment of clear roles and responsibilities for all ICT-related functions, a continuous engagement in the control of the monitoring of the ICT risk management as well in the full range of	Consultation requirement	DORA Chapter II – ICT Risk Management, Section I, Article 4

[10] BCBS sets out seven key principles for operational resilience. Typically adopted by global regulators, their approach is noteworthy. However, this paper is not directly applicable to the majority of the IA's members. For further information see 'Principles for operational resilience' Consultative document, BCBS (https://www.bis.org/bcbs/publ/d509.htm).

[11] The European Commission initiative proposes six areas in which digital operational resilience can be achieved, through oversight, testing and risk management procedures of information communication technology (ICT) risks and incidents. This proposed act is specifically focused on IT and IT supplier resilience, and will not be in force for several years. However, it demonstrates the European regulatory direction of travel with respect to resilience. For further information see 'Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector', European Commission (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595).

[12] The US Joint Authorities' paper details seven key sound practices to be enforced to achieve operational resilience. This paper is applicable for larger global IA member firms and major service provider groups such as custody banks and fund administrators. These sound practices are heavily based on the BCBS principles and are the first public adoption by a major regulator. For further information see 'Sound Practices to Strengthen Operational Resilience', Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency joint paper (https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf).

	approval and control processes and an appropriate allocating of ICT investments and trainings.		
	Firms should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant information to users on a timely basis in order to fully support and facilitate the delivery of the bank's critical operations.	Consultation principle	BCBS – Principle 7
People and culture: the strategy, principles and cultural elements that operationalise good governance	Firms' senior management should implement an approach cognisant of the expectations and allocate resources appropriately.	Consultation principle (BCBS) Consultation requirement (DORA)	BCBS Principle 1 DORA Chapter II – ICT Risk Management, Section I, Article 4
Enabling processes: key activities within a member firm which enable good governance such as policies, procedures and MI generation	Firms should provide an oversight of important business services, mapping, setting impact tolerance, testing and investment decision-making.	Consultation requirement	FCA – Chapter 7 PRA – Chapter 4 DORA Chapter II – ICT Risk Management, Section I, Article 4
	Firms should complete self-assessment document annually (or where there are material changes that might impact operational resilience) and should be reviewed by the board.	Consultation requirement	FCA – Chapter 7 PRA – Chapter 4
	Firms should have appropriate MI to inform board decision-making on operational resilience, and collectively have adequate knowledge, skills and expertise.	Consultation requirement	FCA – Chapter 7 PRA – Chapter 4 DORA Chapter II – ICT Risk Management, Section I, Article 4
	Firms should complete timely insights and reporting to enable effective board oversight, especially with respect to risks and issues.	Consultation principle	BCBS Principle 1
	Firms should conduct lessons learnt exercises to identify, prioritise, and invest in their ability to respond and recover from disruptions as effectively as possible.	Consultation requirement	FCA – Chapter 7
	Firms should have in place measures allowing monitoring the effectiveness of the implementation of their digital resilience strategy as well as bespoke communications plan enabling a "responsible disclosure of ICT-related incidents or major vulnerabilities".	Consultation requirement	DORA Chapter II – ICT Risk Management, Section I, Article 4
	Firms should ensure the lead overseer assesses whether each critical ICT third-party service provider has in place comprehensive governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling an effective ICT risk management.	Consultation requirement	DORA Chapter V – Managing of ICT Third-Party Risk, Section II, Article 30
Subject matter: key topics and areas of focus that should be directed, evaluated and monitored	Firms' self-assessment should contain a written record of: • The firm's important business services and justification for the scoping decisions made. • The associated impact tolerances and justification for the level at which they were set. • The firm's approach to mapping of important business services. • The firm's testing plan and rationale for the plan and scoping decisions. • Details of scenario testing carried out against impact tolerances. • Lessons learned exercises conducted. • The vulnerabilities identified that threaten the firm's ability to deliver important business services within impact tolerances, including actions taken or planned. • Communication strategy and consideration of mitigation of harm. • Methodology used to undertake the above.	Consultation requirement	FCA – Chapter 7

	Firms should refer to existing expectations relating to managing operational risk, cybersecurity, outsourcing and business continuity management such as those within the FCA's Principles for Business (PRIN), Threshold Conditions Sourcebook (COND) and Senior Management Arrangements, Systems and Controls (SYSC).	Consultation principle	FCA – Chapter 1 and Annex 4
	Firms should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.	Consultation principle	IOSCO Principle 1[13]
	Firms should enter into a legally binding written contract with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task to the business of the regulated entity.	Consultation principle	IOSCO Principle 2
	Firms should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.	Consultation principle	IOSCO Principle 3
	Firms should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients, from intentional or inadvertent unauthorised disclosure to third parties.	Consultation principle	IOSCO Principle 4
	Firms should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.	Consultation principle	IOSCO Principle 5
	Firms should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.	Consultation principle	IOSCO Principle 6
	Firms should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.	Consultation principle	IOSCO Principle 7

[13] IOSCO sets out seven key expectations for regulated entities that outsource functions, processes and systems. The paper highlights governance as a key area for consideration when selecting a potential third-party service provider. These principles are based on a joint project between the IOSCO board and committees, including secondary markets, regulation of financial intermediaries, and credit-rating agencies and derivatives, with the aim of assessing whether the existing principles for outsourcing remained suitable, and whether any updates were necessary. For further information see 'Principles on Outsourcing' Consultation Report CR01/2020, IOSCO (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf).

INVESTMENT ASSOCIATION

Pauline Hawkes-Bunyan, Director, Business: Risk, Culture and Resilience

phb@theia.org

John Allan, Senior Operations Specialist

john.allan@theia.org

Clara de Montfort, Assistant Policy Adviser

clara.demontfort@theia.org

EY

James Rounds, Partner, Wealth and Asset Management Operational Resilience Lead, Ernst & Young LLP

jrounds@uk.ey.com

Ali Kazmi, Partner, Financial Services Operational Resilience Lead, Ernst & Young LLP

akazmi@uk.ey.com

Will Ellis, Financial Services Operational Resilience, Ernst & Young LLP

wellis@uk.ey.com

Oscar Knowles, Financial Services Operational Resilience, Ernst & Young LLP

oscar.knowles@uk.ey.com

The Investment Association

Camomile Court, 23 Camomile Street, London, EC3A 7LL

www.theia.org

@InvAssoc