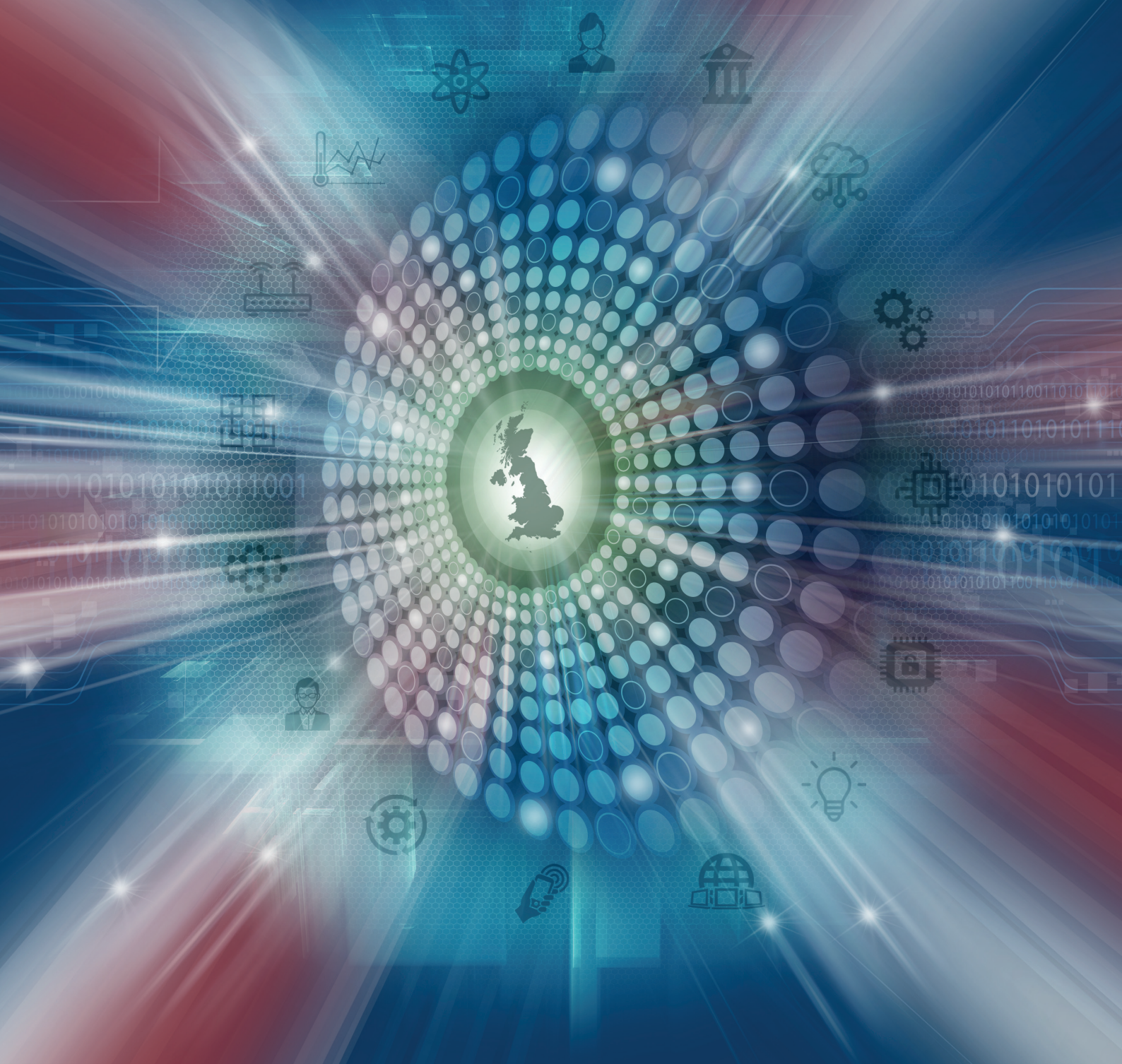


# OPERATIONAL RESILIENCE IN FINANCIAL SERVICES

## TIME TO ACT



## About TheCityUK

---

TheCityUK is the industry-led body representing UK-based financial and related professional services. In the UK, across Europe and internationally, we promote policies that drive competitiveness, support job creation and ensure long-term economic growth. The industry contributes over 10% of the UK's total economic output and employs 2.3 million people, with two thirds of these jobs outside London. It is the largest tax payer, the biggest exporting industry and generates a trade surplus almost equivalent to all other net exporting industries combined.

## About PwC

---

At PwC, our purpose is to build trust in society and solve important problems. PwC is a network of firms in 158 countries with over 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.co.uk](http://www.pwc.co.uk)

# CONTENTS

<b>FOREWORD</b>	4
<b>EXECUTIVE SUMMARY</b>	5
<b>RECOMMENDATIONS</b>	7
<b>INTRODUCTION: THE RESILIENCE IMPERATIVE</b>	9
Defining operational resilience	9
<b>KEY THREATS TO OPERATIONAL RESILIENCE</b>	12
Technological innovation	13
Managing change	14
The menace of cyber attacks	15
The threat of climate change	17
<b>THE AGE OF INNOVATION: HOW NEW IDEAS CREATE RISKS AND OPPORTUNITIES</b>	19
How firms are responding	20
Market composition is changing	20
Recommendations	23
<b>THE ROLE OF GOOD GOVERNANCE</b>	25
Defining governance	25
Organisational structures	26
Management information	29
Culture, skills and capabilities	30
Recommendations	32
<b>REGULATION AND SUPERVISION: A SHIFTING LANDSCAPE</b>	35
A flexible, judgement-led approach	38
The importance of coordination	39
International consistency and cooperation can help	41
Recommendations	42
<b>A CONNECTED WORLD: SYSTEMIC IMPLICATIONS</b>	44
Cross-sector collaboration and testing	46
Substitutability	46
Suppliers and service providers	48
Operating models and concentration risk	49
Recommendations	50
<b>CONCLUSION</b>	53
<b>APPENDIX - OPERATIONAL RESILIENCE FRAMEWORK</b>	54



# FOREWORD

The UK is a world-leading financial and related professional services centre. Its success has been built on innovation, the embracing of new technology and an entrepreneurial spirit which continues to drive competition and excellence. Its open approach to regulation is also a key contributor and the UK is world renowned for offering a safe space for innovation in this area - something which is now being mirrored by other regulators across the world.

Operational resilience is the latest example of the UK regulators blazing a trail. This report presents the first collection of recommendations for industry and regulators which we believe will help to ensure that the UK remains at the forefront of global regulation innovation and a world-leader in financial and related professional services into the future.

Ten years on from the financial crisis, UK institutions are in good shape with strong reserves of capital and levels of liquidity well able to meet the most stringent stress tests. As a result, regulators are shifting their attention towards rapidly emerging economic and operational risks, including culture, governance, and new technology.

Thousands of businesses and millions of customers rely on the industry to save, borrow, purchase products and services and go about their everyday activities with the confidence that the system will work seamlessly. Ensuring this will remain one of the greatest challenges the industry faces in the years to come. Risk factors impacting business operations have grown exponentially in recent years, with increasing examples of cybercrime, hacking and highly sophisticated digital attacks on systemically important firms or institutions. These challenges are compounded by the fact that many institutions have legacy core banking or IT systems in need of updating, and exposure to unpredictable events such as failing infrastructure, extreme weather or natural disasters. All of these factors can impact the capability of individual firms and the industry to maintain critical business services and often such challenges will arise simultaneously and without warning.

How senior leaders deal with these events and how their businesses recover and protect customers and clients will determine their ability to maintain trust and reputation. Critically, a key insight from this report is that operational resilience is a commercial imperative. A firm which can display to its shareholders, clients and customers that it can maintain core services safely and efficiently through or despite of an operational disruption or crisis will gain market advantage, promote the UK internationally and be more sustainable over the long term. Those which cannot, may not last very long.

This report was jointly produced by TheCityUK and PwC. Its production has been made possible by the willingness of senior leaders and practitioners from across the industry to give their time and insights. In total, over 30 financial and related professional services firms have been interviewed for this report. I would like to thank everyone who has been involved in this project for their support. Special thanks are in particular due to the team at PwC for their work and support in developing these recommendations, the first of their kind in this space.



**Miles Celic**

Chief Executive Officer, TheCityUK



# EXECUTIVE SUMMARY

As the leading global financial centre and number one exporter of financial services, the UK economy as a whole - not just individual customers and employees - relies on financial services continuing to operate uninterrupted.

Digitalisation is transforming financial services and many firms are sitting uneasily between a digitally-driven future and the legacy systems of the past. Firms are embracing innovation and connecting with customers and others across multiple channels. New entrants are leveraging technology to offer niche products and services and to create Application Programming Interface (API)-enabled ecosystems of interconnected companies. Meanwhile, to embrace technology and become agile, firms are moving to the cloud and other forms of outsourcing, which adds to the complexity. Vital elements of key business services are now being delivered by companies outside the regulatory perimeter, often concentrated among a few major providers. Adoption of public cloud services - rare just two years ago - is becoming increasingly common.

However compelling the reason for change, embarking on change can also be a source of risk, as well as a cause of interdependence and a threat to stability. In addition, external threats are increasing. Cyber attacks, for example, are becoming more frequent and more sophisticated, and climate change may soon also drive greater uncertainty.

Threats to future financial stability and businesses over the coming decades will be complexity, connectedness, and criminal activity, all of which have the potential to disrupt services to customers and undermine financial stability. Disruption at a scale that threatens the viability of one or more major financial services firm has moved from unlikely to comprehensible, and now to inevitable.

The good news is that the very actions that need to be taken to be resilient are those that can create a genuinely customer-centric, adaptive, data driven and simplified firm. The opportunity to rebalance the traditionally siloed functional view of a firm, to an end-to-end view, driven by customers and linked to the purpose of the firm, is significant.

Firms must urgently address the changes required to their business to improve their ability to foresee, prevent, detect and recover from operational disruptions. The difficult questions that remain are how much more needs to be done, and how much is enough?

It remains the case that often those firms with the most robust approach to resilience and recovery have learnt the hard way - through their own 'near death' experience. Recent years have seen a number of cases of loss of reputation, reduced enterprise value and senior executive casualties from operational incidents that have been badly handled.

In response to these challenges, regulators are becoming increasingly concerned with operational resilience and are stepping up their activities. In July 2018, the Bank of England (BoE), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) published a discussion paper<sup>1</sup> to share their thinking and invite feedback. Their starting point was that operational disruptions have the potential to harm consumers and market participants, threaten firm viability, and cause instability in the financial system.

Regulation has an important role to play but action also needs to come from the industry itself and there is a compelling business imperative to address these issues. To maintain market share, build trust and embrace innovation, operational resilience needs to be prioritised and invested in. But, in contrast to the investments already made across financial services to address financial resilience, the cost of achieving operational resilience will be small, often incremental and will bring with it significant opportunities.

1 Bank of England, Prudential Regulation Authority, Financial Conduct Authority, 'Building the UK financial Sector's Operational Resilience', Discussion Paper, (July 2018), available at: <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>

PwC and TheCityUK have responded to these challenges and developed a range of recommendations for both the regulator and the industry after extensive interviews with over 30 senior executives across the financial services sector. These recommendations will help make the UK-based industry, and the economy, more secure, globally competitive and sustainable.

### Key Findings

- In an era of transformation, there is a strong business imperative to invest in operational resilience. Certainly, if firms are able to withstand disruptive events they are more likely to innovate safely and maintain the trust of their customers.
- Embracing greater integration without resolving complexity makes resilience more difficult to achieve.
- Governance and, in particular, the culture of an organisation, play a key role in maintaining operational resilience.
- For a global financial services centre, operational resilience cannot be achieved without international consistency and cooperation.
- There is both a need and appetite for more cross-sector collaboration to support resilience.
- It is clear there is no one size fits all approach to building resilience. Instead firms need to reflect on their own risk positions, resources, systemic importance, and impact on others.

# RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS

## The age of innovation

1. Adapt risk frameworks, governance and strategy to keep pace with the innovation agenda.
2. Tackle the potential for disruption head on by reviewing the approach to change.
3. Routinely address resilience of key services in determining both strategy and investment in systems, including approach to legacy systems.
4. Build operational resilience into strategy and business plans, reflecting growth trajectories and systemic importance.

## Target



## The role of good governance

5. Develop a clear view of a firm's purpose and place in the context of the wider economy when establishing governance arrangements.
6. Establish individual accountability and collective responsibility to better support resilience decision making by extending existing regulatory tools and governance structures.
7. Establish comprehensive end-to-end management information and reporting for important business services.
8. Encompass operational resilience skills and capabilities in management development programmes.
9. Be more transparent about the threats to the ongoing delivery of important business services through more detailed external disclosures and regulatory reporting.

## Target



# RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS

## Regulation and supervision

10. Continue to take a lead role in driving consistent global regulatory standards.

### Target



11. Provide greater clarity to firms on how to govern and manage operational resilience where there are already existing initiatives that overlap.



12. Enhance supervisory capabilities by expanding skills and experience.



## A connected world

13. Find collective solutions to common challenges by establishing cross-sector initiatives around scenario testing, stress testing and information sharing.

### Target



14. Address the potential for 'firm paralysis' by integrating recovery and resolution and cyber arrangements across the sector.



15. Map the sector and its dependencies to understand systemic operational interdependencies. This could include reconsidering the regulatory perimeter.



16. Work with technology and other providers to develop standardised support frameworks and opportunities for substitutability of key infrastructure services.



17. Overhaul supplier management frameworks to improve operation of key third-party provided services.





# INTRODUCTION: THE RESILIENCE IMPERATIVE

UK-based financial services firms are transforming amid new technologies, shifting customer behaviours and changing political realities. There is a sense of uncertainty, but also of creative disruption that is shaping a more dynamic business environment.

Firms are investing for the future. In new IT platforms, data and advanced analytics they see the chance to sharpen performance and align with the regulatory agenda. A diverse group of new entrants is bringing innovation, supported by technologies that enable smarter, faster delivery. With the help of digitalisation, the industry is poised to embrace the opportunities presented by an increasingly connected global economy.

However, as much as technology is an enabler of change, the change process is often complex, expensive and dysfunctional. Few firms have managed to develop a strategic agenda to match their technological ambition, and the competitive temperature is rising. A new generation of FinTechs comes unencumbered with legacy IT systems creating an environment which increases competitive pressure. Implementation of change programmes brings the risk of IT failures, outages and misspent budgets. Outsourcing boosts connectivity, but in turn increases third-party and related concentration risk. Where there are limited choices, this can build concentration with a knock-on increase in systemic risk of certain firms. Integration and transformation project timelines, particularly for addressing legacy are long and can hamper a firm's agility and ability to adopt new technology. Finally, digitalisation has encouraged a new kind of market participant. Cyber criminals, malign state actors and hackers hover on the fringes, targeting weakness and aiming to profit from superior technical expertise.

In the Bank of England's (BoE) latest systemic risk survey, some two thirds of respondents cited cyber attacks as a key source of risk.<sup>2</sup>

Operational disruptions from cyber, change programmes or other causes have the potential to harm financial services firms, consumers and other financial market participants. In some cases they threaten viability and lead to instability in the wider financial system. To combat these challenges regulators are increasingly focused on ensuring that firms are operationally resilient; that they are reasonably able to guarantee the continuity of their most important business services, and adapt to unexpected events or sudden disruption. Achieving resilience relates to an outcome rather than a specific set of requirements. It will differ depending on a firm's critical functions, business model and operational priorities.

## Defining operational resilience

As the industry engages with operational challenges, regulators are working to promote understanding of the potential impact of failures, and to better equip firms to manage disruption. The BoE in 2015 described resilience as: "An organisation's ability to protect or sustain its critical functions, and underlying assets, while adapting to expected or unexpected occurrences of operational stress or disruption."<sup>3</sup> The BoE's approach was notable for its focus on critical functions and the importance of agility, anticipation and response.

Over time, policymakers have worked to evolve their definition. The BoE has described operational resilience as: "The ability to adapt operations to continue functioning, when – not if – circumstances change."<sup>4</sup> The BoE's interpretation is useful because it recognises the inevitability of adverse events. Indeed, a challenge for firms is that operational failures are unavoidable.

2 The Bank of England, 'Systemic Risk Survey Results - 2018 H1', (June 2018), available at: <https://www.bankofengland.co.uk/systemic-risk-survey/2018/2018-h1>

3 The Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, 'Building the UK financial sector's operational resilience discussion paper', (July 2018), available at: <https://www.fca.org.uk/news/press-releases/building-uk-financial-sector%E2%80%99s-operational-resilience-discussion-paper>

4 Charlotte Gerken, Director, Supervisory Risk Specialists at the BoE, speech at the Operational Risk Europe Conference, (June 2017), available at: <https://www.bankofengland.co.uk/-/media/boe/files/speech/2017/the-boes-approach-to-operational-resilience.pdf>

**“[Firms should]...be on a WAR footing, withstand, absorb, recover.”<sup>5</sup>**

Lyndon Nelson, Deputy CEO of the PRA and Executive Director BoE

The joint BoE, PRA, FCA discussion paper ‘Building the UK’s financial sector’s operational resilience’<sup>6</sup> published in July 2018, defines operational resilience as: “The ability of firms, financial market infrastructure (FMIs) and the sector as a whole to prevent, respond to, recover and learn from operational disruptions.” This expands on the earlier concept, highlighting the importance of learning lessons as an essential part of engaging with this agenda.

A major theme in this report is that the key aim of operational resilience should be the continuation of business services. This represents a shift in focus away from considering the preservation and the interests of shareholders, to a firm’s ability to understand the impact on customers and other stakeholders. The report sets out how firms can set thresholds (‘impact tolerances’) for the continuity of important business services. Their ability to meet these targets can then be tested. The regulators also see a business services approach as an effective way to prioritise improvements to IT systems and business processes.

PwC’s work in this area suggests firms that have experienced disruption previously are often more resilient than those that have not. However, the challenge for regulators and the industry is to facilitate learning before the event. The BoE Financial Policy Committee’s (FPC) introduction of cyber stress testing, announced in June 2018, is a good example of the importance supervisors place on this aspect.

PwC and TheCityUK conducted over 30 interviews to inform this report in which industry executives reflected beyond the established prevent, respond, recover process to also consider the ‘how’. Key themes that arose in our discussions include the unexpected and varied forms that disruption can take, the importance of culture in building resilience, the key role played by management information, and the attractiveness of resilience by design.

A universal theme arising from these interviews was that operational resilience is an important topic that is here to stay.

**“Operational resilience is not an enabler; it is a core investment. Operational resilience is part of what we are.”**

Interviewee

With these sentiments in mind, TheCityUK and PwC would like to suggest their own definition of resilience: “The embedding of capabilities, processes, behaviours and systems, which allow a firm to continue to carry out its mission in the face of disruption regardless of its source.”

Critically, TheCityUK and PwC view operational resilience as an outcome, not an individual function, process or department.

Finally, PwC is very grateful to those who have taken the time to share their thoughts and perspectives, and hope our joint work will encourage continued dialogue and debate.

<sup>5</sup> Lyndon Nelson, Deputy CEO of the PRA and Executive Director BoE, in a speech entitled: ‘Resilience and continuity in an interconnected and changing world’ – 20th Annual Operational Risk Europe, (June 2018), available at: <https://knect365.com/riskminds/article/d752998f-89dc-4f46-9bb8-2542695489f3/becoming-operationally-resilient-the-past-present-and-future-for-financial-services>

<sup>6</sup> The Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, ‘Building the UK financial sector’s operational resilience discussion paper’, (July 2018), available at: <https://www.fca.org.uk/news/press-releases/building-uk-financial-sector%E2%80%99s-operational-resilience-discussion-paper>

**Figure 1:** Operational resilience key domains

Source: PwC



There are a number of disciplines and regulatory initiatives relevant to operational resilience that are sometimes confused with it. Among the most notable is cyber security. Indeed, a breach of cyber security is a significant source of operational disruption. However, a cyber security function alone cannot deliver operational resilience, as this requires alignment across a multitude of functions. Cyber resilience has also become a frequently used term, despite varying and inconsistent descriptions of what it is. Being resilient to cyber attacks requires a broad set of capabilities, many of which are not specific technical cyber capabilities.

Operational Continuity in Resolution (OCIR), meanwhile, is part of a broader set of recovery and resolution planning requirements set out by the PRA. It aims to ensure that critical economic functions continue in recovery and resolution. Although there are similarities between the two, operational resilience scenarios are different – for example, focusing on supporting business as usual, as well as recovery and resolution.

Operational risk also shares characteristics with operational resilience. The difference is that operational risk (usually in the prudential context) addresses the risk of loss from an event, while operational resilience is concerned with whether a firm reacts appropriately when a risk crystallises, recognising that additional capital is unlikely to mitigate the risks.

Given the broad scope of operational resilience, the first challenge is to ensure that it is well understood across the industry. Its meaning will continue to evolve as new risks, technologies and business models emerge, but establishing a common view and response infrastructure will support the financial services sector in adapting effectively.

# KEY THREATS TO OPERATIONAL RESILIENCE

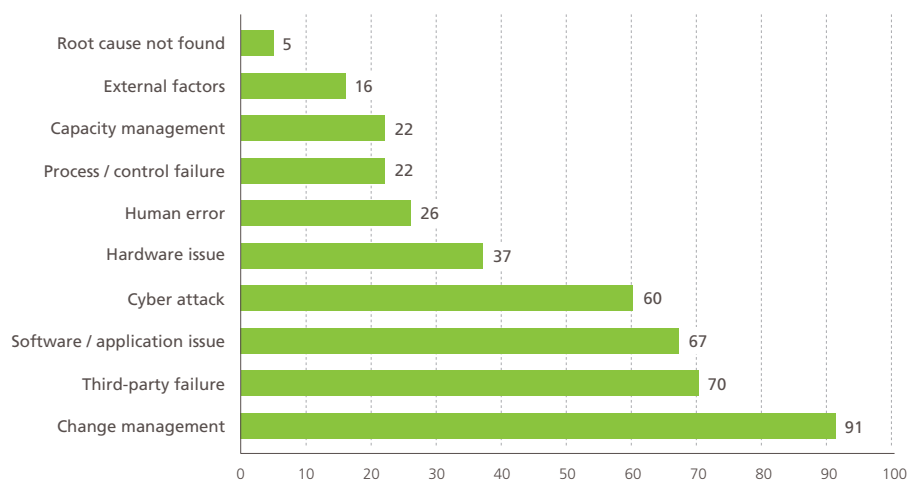
- The speed of technological innovation and the rapid adoption of new, less established technologies is increasing the risk of disruption.
- Firms' approaches to managing change and investment will play a crucial role in developing resilience.
- Cyber threats are rising and the impact of attacks is increasingly likely to be significant.
- Climate change will test resilience to physical risks and disrupt operations through changes in market sentiment and economic models.
- Fraudsters, often cyber enabled will seek to exploit weaknesses when firms experience operational difficulties.

In an increasingly connected and digitalised financial system, the threat of operational disruption is ever more acute. Firms face a range of risks to business as usual that include IT renewal programmes, cyber attacks, and the impacts of evolving relationships with third parties.

In November 2018 the FCA published a survey of technology outages in UK financial services, which showed that the number of incidences had more than doubled over the previous year.<sup>7</sup>

**Figure 2:** Overview of technology outages report to the FCA (2017-2018)

**Source:** Financial Conduct Authority, 'Cyber and technology resilience: themes from cross-sector survey 2017-2018', (November 2018)



As illustrated in this survey, UK regulators are particularly focused on technology. The industry is allocating significant investment to new platforms, analytics and digital services, and these create complexity and carry implementation risk. At the same time, companies face an increasingly hostile environment.

Another source of risk is increasing reliance on third parties, a symptom of the explosion of FinTechs, alongside a trend toward outsourcing and the nascent growth of ecosystems and API-driven partnerships.

Third-party incidents accounted for 15% of operational incidents reported to the FCA in the year to September 2018 (the second highest cause).

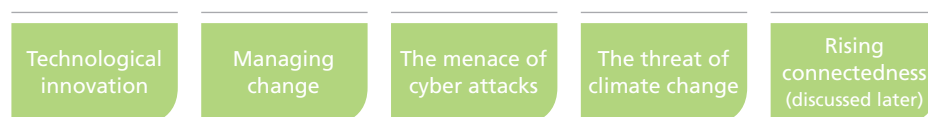
<sup>7</sup> Financial Conduct Authority, 'Cyber and Technology Resilience: Themes from cross-sector survey 2017-2018', (November 2018), available at: <https://www.fca.org.uk/publications/research/cyber-technology-resilience-themes-cross-sector-survey-2017-18>

A related issue is the proliferation of distribution channels for financial products and services, a trend likely to accelerate as Open Banking becomes established in the UK and globally.

Other threats are less immediate. Climate change may not have flashed red on the risk radar historically, but PwC is seeing a shift in attitudes led by the Network for Greening the Financial System (NGFS) with central bank and regulator representation.<sup>8</sup> Warmer temperatures and more frequent severe weather events can have numerous impacts. These range from physical damage to pressure on business models arising from factors such as changing consumer behaviours and regulatory initiatives.

In addition, there are numerous less likely threats, such as the impact of terrorism, epidemics and energy outages. And at the margin, unexpected events (so called black swans) are especially hard to predict. As has been shown in recent history, however, such events do occur.

The FCA asked firms to explain the reasons for the failures, which, together with the interviews for this report, lead to the identification of five areas of threat listed below, with the exception of connectedness, which is discussed in detail later in the report.



## Technological innovation

The financial services sector globally is an innovation leader. Banks, insurers, asset and wealth managers and others are increasingly automated front-to-back, often leveraging advanced analytics to make decisions and interact more effectively with customers. The Open Banking regulatory initiative is enabling customers to require that transaction data is shared, leading to the emergence of a new generation of payment and account-related services. Companies such as Tencent and Alipay are leading a revolution in the development of ecosystems in which thousands of companies coalesce around a single point of entry. Thousands of FinTechs, meanwhile, are building businesses by targeting niche links in the value chain, often partnering with established firms to do so. Technology companies are attracting hundreds of millions of dollars of investment and employing thousands of people.

The cloud, artificial intelligence (AI), robotics and blockchain were less developed just a few years ago. Now AI applications, machine learning and robotic process automation are helping firms streamline models, processes and operations. Complexity is increasing, leading to multiple dependencies that are neither transparent nor regulated. This has increased the chance that a small supplier sitting outside the regulatory perimeter becomes a key point of vulnerability.

The pace and ambition of innovation is helping the industry address areas of historic under investment. However, there is a flipside. A growing dependence on technology and the complexity of an interconnected world bring challenges. Firms must make sure that data is available, accurate and confidential, and they must comply with an ever-growing roster of cyber and privacy regulations. Outages can lead to significant operational breakdowns, and more connectedness raises the chance, and potential impact, of a systemic event.

<sup>8</sup> Bank of France, 'A call for action: Climate change as a source of financial risk', (April 2019), available at: [https://www.banque-france.fr/sites/default/files/media/2019/04/17/synthese\\_ngfs-2019\\_-\\_17042019\\_0.pdf](https://www.banque-france.fr/sites/default/files/media/2019/04/17/synthese_ngfs-2019_-_17042019_0.pdf)



In some cases, firms are adopting relatively new technologies. Certainly, the implications of changes may not be fully understood, and innovation may be a direct root cause of new vulnerabilities and unquantified exposures for clients and consumers.

Through mergers and divestments, the UK financial services sector, and particularly banking and insurance, has seen significant structural change in the past decade. The integration challenge presents a considerable risk to resilience, which requires being able to continue to provide important business services.

One common consequence of rapid technology change is a lack of alignment between the business and technology, with senior individuals often unable to provide appropriate levels of challenge. Equally, investment decisions may be taken by IT specialists who do not have sufficient insight into the firm's business objectives.

Finally, the industry faces a relative scarcity of skills and experience. Without the right capabilities, there is a risk that firms make poor decisions.

According to PwC's Global FinTech Report 2017<sup>9</sup>, some 80% of firms (FinTechs and incumbents) struggle to hire and retain people with the required skills for innovation.

## Managing change

Financial services firms face a proliferation of threats to operational resilience arising from business model evolution, IT infrastructure renewal, and the changing competitive and regulatory landscape. Indeed, change management was the number one root cause of operational incidences highlighted in the FCA's recent survey.<sup>10</sup> TheCityUK and PwC see four key sources of change-related risk, each of which carries significant disruptive potential:

- **New products and services.** Innovation, performance targets and competition require firms to adjust their strategies and business models continually. Many firms are adopting agile strategies, encouraging rapid and flexible development cycles. These require careful planning, arguably with a greater need for governance and process discipline than the traditional sequential design 'waterfall' approach. In addition, the siloed nature of some IT infrastructures means they are not set up to accommodate agile development, which can increase risk around delivery.
- **Technology upgrades (and legacy systems).** IT upgrades, re-platforming and software development are often at the leading edge of change programs, and many firms are implementing technology-driven changes across the business. As they do so, they often must contend with numerous legacy systems and databases, which run in parallel with legacy organisational structures. This creates complexity in managing change and risk to delivery. IT changes alone caused 20% of operational incidents between October 2017 and September 2018, based on reports to the FCA.<sup>11</sup>
- **External environment.** External events, such as Brexit, can have a significant impact on operations, as firms switch to new locations or reconsider long-term projects. These moves impact areas including IT, risk management, people and premises.

<sup>9</sup> PwC, 'Global FinTech Report 2017', (November 2017), available at: <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2017.pdf>

<sup>10</sup> Financial Conduct Authority, 'Cyber and Technology Resilience: Themes from cross-sector survey 2017-2018' (November 2018), available at: <https://www.fca.org.uk/publications/research/cyber-technology-resilience-themes-cross-sector-survey-2017-18>

<sup>11</sup> Ibid.

- **Regulatory policy and change.** Firms are challenged because policymakers have previously focused their efforts on driving financial resilience and better conduct, rather than on the operational impacts of new rules. PwC's recent work with financial firms suggests that the scale and complexity of regulatory change projects continues to exert operational pressure. Furthermore, there have been a number of recent examples of regulators requiring firms to provide detailed explanations of their change portfolios and methodologies. Intense regulatory scrutiny ensures these projects remain at the top of the C-suite agenda.

These examples illustrate that change, and the management of change, are indeed significant threats to operational resilience. On the other hand, a failure to change may arguably be a bigger threat in the longer term. The strategic task for firms is to effectively balance the need to change, against the risks associated with the change process.







## The menace of cyber attacks

Cyber attack is consistently cited as the single most urgent concern among senior industry executives. The sentiment is also reflected in official surveys. A BoE Systemic Risk Survey published in 2018, showed 66% of respondents cited cyber security as a key source of risk, up from 55% a year previously.<sup>12</sup>

There have been a number of incidents in the recent past that have fuelled this concern.

**Figure 3:** Examples of recent financial services incidents

Source: PwC

	Generic threats	Financial services
<b>Key cyber threat scenario</b>	  <p>Ransomware encrypting data and disrupting business operations.</p> <p>Reliance on internet service providers, which are disrupted.</p>	    <p>Disruption of online services to create market volatility and damage reputation.</p> <p>Theft of funds from individuals and institutions by hacking payment services.</p> <p>Theft of sensitive commercial information to manipulate markets.</p> <p>Theft of personally identifiable information to defraud individuals.</p>
<b>Recent examples</b>	<p>WanaCryptor ransomware infects organisations via trusted third-party application.</p> <p>Distributed denial of service attack on DNS provider disrupts internet traffic to organisations like Amazon and PayPal.</p>	<p>Distributed denial of service attacks aimed at online banking services or time critical price sensitive market data feeds.</p> <p>Malware attack on banks' messaging channel or their customers' online banking sessions.</p> <p>Insider theft of proprietary trading algorithms or market sensitive M&amp;A data.</p> <p>Hack of customer web application to access customer database and exfiltrate personally identifiable information.</p>

12 Bank of England, 'Systemic Risk Survey Results - 2018 H1', (June 2018), available at: <https://www.bankofengland.co.uk/systemic-risk-survey/2018/2018-h1>

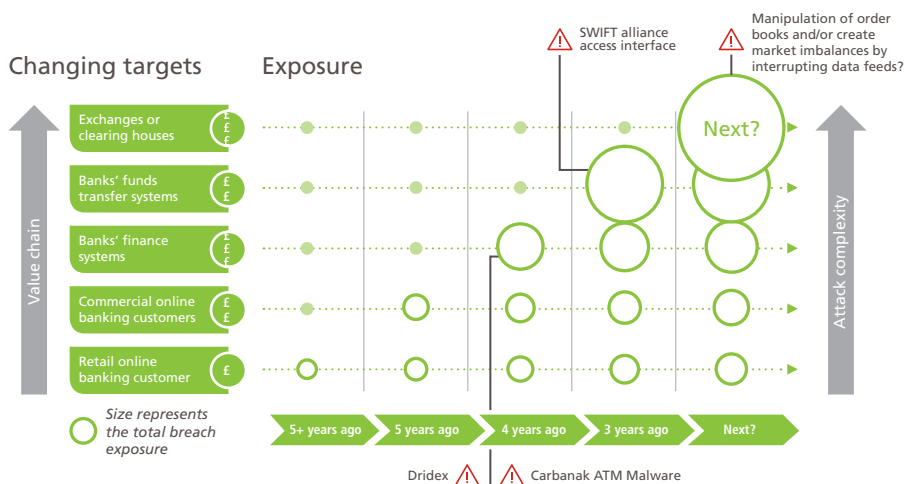
One reason for the increasing threat of cyber attacks is accelerating connectivity in the financial services ecosystem, which has led to a proliferation of digital touchpoints. All of these offer windows of opportunity for attackers. Rising numbers of attacks over the recent period have been against the infrastructure of the internet - for example controls, routers, and switches, where bad actors see a chance to manipulate traffic.

Attacks are going deeper and becoming more sophisticated. TheCityUK and PwC expect that trend to continue, with attackers using more complex strategies and focusing on the most valuable targets.

**Figure 4:** Changing nature of cyber attacks

Source: PwC

**Note:** Cyber attacks are expected to move upwards into more valuable targets within the banking ecosystem through using increasingly complex methods



One of the challenges firms face in combating cyber risk is that threats come from numerous diverse sources that represent varying motivations and objectives. These may be hacktivists looking to make a political point, organised criminals motivated by financial gain, or nation states seeking intelligence or disruption.

Points of exposure to cyber attack are arguably even more diverse. They include the following:

- **internal IT:** core systems, laptops, software and development technologies
- **counterparties/partners:** close partners or non-contractual single points of failure such as messaging services
- **outsourced providers:** cloud providers and FinTechs that are increasingly targeted as the weak link to get access to regulated firms and data
- **supply chains:** complex supply chains could result in concentration risk in a country or particular company that is providing services to a number of parties in the same supply chain
- **disruptive technologies:** cloud services and Internet of Things (IoT), which widens the 'attack surface' and creates uncertainty around the perimeters of networks
- **infrastructure:** IT networks, payments networks and power services
- **externalities:** international conflicts and malware pandemics.

Cyber risk shares many of the attributes of the circumstances that led up to the financial crisis. These include individual firms considering their risks in isolation rather than systemically, complexity of systems and a lack of appreciation of interdependencies. There is also a common lack of understanding at board level of some technologies and advanced digital systems.<sup>13</sup> The FCA's wholesale banks and asset management cyber multi-firm review findings shows a large number of board members and non-IT senior management are unable to discuss cyber issues coherently, clearly explain cyber risks, or provide effective challenge.<sup>14</sup> The findings highlight that just 47% of firms provide additional training to high-risk staff. It also evidences a general failure to link between cyber and other conduct issues. For example, firms do not generally consider that cyber attacks may be motivated by attempts to commit market abuse or financial crime.

The second line of defence – including risk and compliance functions – also has limited technical cyber expertise, according to the FCA's publication<sup>15</sup>. In fact, the size of technology risk functions has decreased relative to the size of organisations since 2016, according to a recent PwC report.<sup>16</sup> Without that capacity and knowledge, firms are limited in their ability to test and challenge the tasks across the first line of defence (the business itself).

## The threat of climate change

Climate-related risks have the potential to cause significant disruption and reputational damage. There are two key areas to consider: physical and transition risks.

Physical risk can arise from extreme weather events such as storms, floods and heatwaves, as well as longer-term changes such as gradual increases in temperatures and rising sea levels. These can lead to threats to physical assets and data, as well as disruptions to client services, and are probably the biggest threat in the short-term. Physical risks are likely to be material where assets are located in places at risk of extreme weather events. In September 2018, for example, Typhoon Mangkhut caused severe destruction in South East Asia, damaging offices and IT infrastructure. Impacts were particularly felt in the Philippines, an important location for business process and IT outsourcing. Many experts believe the frequency and intensity of such extreme weather events may increase as global temperatures rise.

<sup>13</sup> TheCityUK and Marsh, 'Governing cyber risk: a guide for company boards', (April 2018), available at: <https://www.thecityuk.com/research/governing-cyber-risk/>

<sup>14</sup> Financial Conduct Authority, 'Wholesale banks and asset management cyber multi-firm review findings', (December 2018), available at: <https://www.fca.org.uk/publications/multi-firm-reviews/wholesale-banks-asset-management-cyber-multi-firm-review-findings>

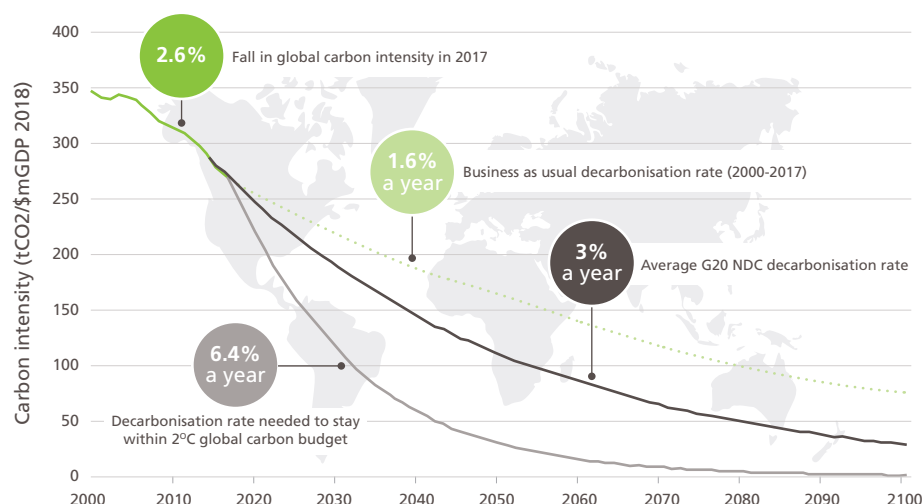
<sup>15</sup> Ibid.

<sup>16</sup> PwC, 'Global Technology Risk Report', (April 2019), available at: <https://www.pwc.co.uk/financial-services/assets/pdf/global-technology-risk-management-study-v2.pdf>

**Figure 5:** Current trends of decarbonisation

**Source:** BP, Energy Information Agency, World Bank, IMF, UNFCCC, National Government Agencies, PwC data and analysis

**Note:** GDP is measured on a purchasing power parity (PPP) basis. The NDC pathway is an estimate of the decarbonisation rate needed to achieve the targets released by G20 countries. NDCs only cover the period to 2030, we extrapolate the trend in decarbonisation needed to meet the targets to 2100 for comparison



Perhaps less obvious are transition risks such as changing market sentiment, or the gradual move towards a lower-carbon economy, which is likely to entail extensive policy, legal, technology and market evolutions. These have the potential to impact firms providing financial services to carbon-intensive companies or industries.

Some firms have suggested they are cognisant of the threats posed by climate risk. Some 60% of banks recognise that climate change is a factor that could increase their operational risk profile, according to a recent PRA survey, especially where key elements in a firm's operations, or wider supply chain, are located in vulnerable areas.<sup>17</sup> Some firms with outsourced functions in at-risk locations have conducted analysis using physical risk scenarios such as those published by the Intergovernmental Panel on Climate Change (IPCC). Firms may increasingly include insured loss data as part of this analysis, as well as examining recent historical climatic trends in key locations.

The recommendations of the Financial Stability Board's (FSB) Task Force for Climate-related Financial Disclosures (TCFD) provide a framework for analysis, with guidance across strategy, governance, risk management, and metrics and targets.<sup>18</sup> This kind of risk identification and management exercise makes good business sense and is increasingly in line with UK regulators' expectations. In a supervisory statement published in April 2019<sup>19</sup>, the PRA suggests that it expects banks and insurers to undertake scenario analysis to identify relevant climate-related risks. The PRA also calls for board-level engagement and accountability, and suggests that firms should identify a senior management function to be responsible for identifying and managing climate-related risks, including operational risks.

<sup>17</sup> Prudential Regulation Authority, 'Transition in thinking: The impact of climate change on the UK banking sector', (September 2018), available at: <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/transition-in-thinking-the-impact-of-climate-change-on-the-uk-banking-sector>

<sup>18</sup> Financial Stability Board's, (FSB) Task Force for Climate-related Financial Disclosures, (April 2015), available at: <https://www.fsb-tcfd.org/>

<sup>19</sup> Bank of England, Supervisory statement SS3/19, (April 2019), available at: <https://www.bankofengland.co.uk/prudential-regulation/publication/2019/enhancing-banks-and-insurers-approaches-to-managing-the-financial-risks-from-climate-change-ss>



# THE AGE OF INNOVATION: HOW NEW IDEAS CREATE RISKS AND OPPORTUNITIES

- While the financial services sector has always embraced innovation, the current speed of innovation is not matched by the depth of understanding at a management level.
- Embracing integration without resolving for complexity raises the stakes in respect of operational resilience.

Innovation is the lifeblood of financial services and is probably the most important issue on many firms' agendas. From IT renewal, to the development of new services, interfaces and back-office systems, firms are striving to become leaner, more efficient and more responsive to the requirements of the business. Innovation is also increasingly being driven by third parties, listed below.

- **FinTech.** Technology-enabled innovation that could result in new business models, applications, processes or products with an associated material effect on financial services.<sup>20</sup>
- **BigTech.** Large technology companies that expand into direct provision of financial services or products very similar to financial products.<sup>21</sup>
- **ServTech.** A discrete category of firm that refers to those that provide for example, infrastructure, platforms and software as a service.

The combined impact of these is accelerating innovation, not least because they have been encouraged by regulatory initiatives such as the European Union's (EU) Payment Services Directive 2 (PSD2).<sup>22</sup> This creates an environment in which innovation is directly connected to an improved customer experience. PSD2 also provides a legal framework for the Open Banking standard, also established by UK regulators. Open Banking is part of a wider trend of giving citizens and customers more control over data, and revitalising competition through modern technologies, processes and business models. It is seen as a key driver of banks' digital strategies.<sup>23</sup>

Another driver of innovation is the dynamics of consumer expectation in response to the growth of innovative delivery models in non-financial services. These expectations typically prioritise convenience, availability, agility and interconnectedness. Finally, cost pressures driven by regulation, low interest rates and competition compel firms to embrace the opportunities that innovation presents. These collective conditions are driving wholesale change at a firm level and in terms of market composition.

20 Financial Stability Board (FSB), 'FSB's Task Force for Climate-related Financial Disclosures', (April 2015), available at: <https://www.fsb-tcfd.org/>

21 Ibid.

22 European Parliament, Directive 2015/2366, (November 2015), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366>

23 PwC & Open Data Institute, 'How to seize the open banking opportunity', (June 2018), available at: [https://retailbankinginnovation.fintecnet.com/uploads/2/4/3/8/24384857/the\\_future\\_of\\_banking\\_is\\_open.pdf](https://retailbankinginnovation.fintecnet.com/uploads/2/4/3/8/24384857/the_future_of_banking_is_open.pdf)

## How firms are responding

At an individual firm level, the opportunities presented by a diverse range of technologies are wide-ranging.

- cutting processing latency and dialling back on manual intervention
- robo-advice in investment management
- robotics and AI in operations and technology functions
- increasing use of platforms in asset management
- using blockchain for payment, settlement and custody.

In fact, firms are pursuing a range of innovation agendas based on multiple methodologies and delivery models. Some are ramping up their use of the cloud. Just three years ago, most firms were sceptical about cloud technology. A year ago, however, many started moving data to private clouds. Today, the use of public clouds is accelerating. This represents a significant shift in attitudes over a short period. Many firms are expanding their distribution options, digitalising front-to-back or partnering up with FinTechs.

At the same time many firms are looking to simplify operationally, based on an end-to-end view of business services.

## Market composition is changing

The opportunities presented by innovation are having a fundamental impact on market composition. New entrants are becoming established rapidly, some seeking licences to operate and others looking to join the financial ecosystem from outside the regulatory perimeter. Many are forming partnerships with incumbents, but may not be considering operational resilience as part of their due diligence. At the same time, a range of utilities are emerging, for example in trading, execution and data management.

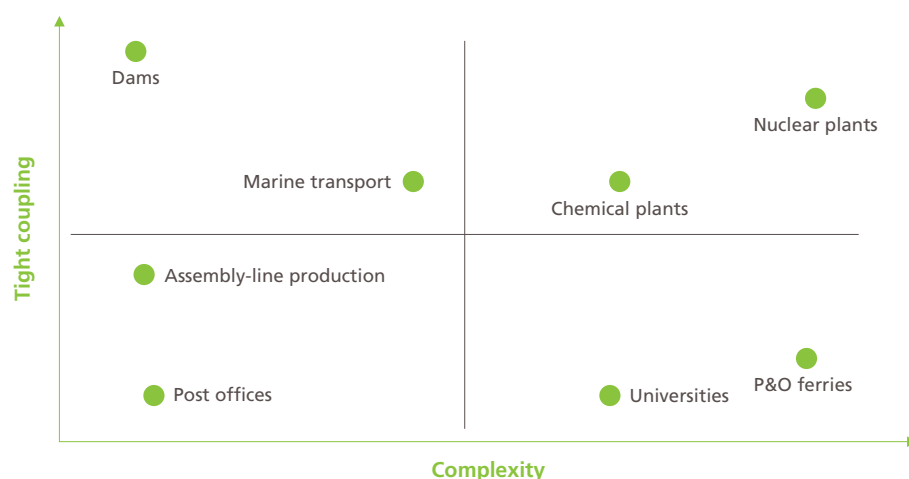
The operational resilience implications are significant. Much has been written about 'tighter coupling' and its relationship with complexity, and the coalescence of both is underway in financial services.<sup>24</sup> This has moved the industry into a 'danger zone', in which predicting, preventing and identifying a potential event has become more challenging.

---

<sup>24</sup> Chris Clearfield & András Tilcsik, *Meltdown: Why our systems fail and what we can do about it* - Atlantic Books (March 2018)

**Figure 6:** Relationship between tight coupling and complexity

**Source:** Chris Clearfield & András Tilcsik, *Meltdown: Why our systems fail and what we can do about it* - Atlantic Books, (March 2018)



A key area of innovation is focused on moving IT activities to the cloud. Offerings such as software-as-a-service and business-process-as-a-service are changing the way in which firms operate. On the one hand, it enhances resilience, for example, through cutting reliance on physical hardware and enabling more collaboration. On the other, it increases concentration risk and therefore the potential impact of an operational event.

In addition, new forms of innovation-led threats are emerging. In one recent example, the death of the Chief Executive Officer of a cryptocurrency exchange led to millions of dollars of losses. The reason was that he was the sole holder of password details and did not keep an accessible record. Here, the security that was perceived to render the currency resilient resulted in an operational crisis.

Another fast-changing area is data management. The financial sector is the custodian for large volumes of valuable personal and transaction data, which is why it is such a popular target for cyber attacks. As more firms join the financial services ecosystem data is becoming an increasingly valuable asset. Resilience is required to protect it.

The global and UK regulatory response to innovation and the impact it is having on the market as a whole is delicately balanced. The FSB hails the 'great promise' of technology to increase market access, product range and convenience, while also lowering cost. But it also warns of the impact it will have on concentration, contestability and composition.

The G20 said, "Transformative technologies are expected to bring immense economic opportunities, including new and better jobs, and higher living standards. The transition, however, will create challenges for individuals, businesses and governments."<sup>25</sup> It calls for international cooperation when designing and implementing policy.

UK regulators describe themselves as 'technology neutral', but they are alive to the challenges, and balance their support with concern over consumer protection and market stability. The new focus on operational resilience is a key element of this.

<sup>25</sup> European Council, 'G20 Leaders' Declaration: building consensus for fair and sustainable development', (December 2018), available at: <https://www.consilium.europa.eu/en/press/press-releases/2018/12/01/g20-leaders-declaration/>

From one perspective innovation and resilience are closely related. Innovation is fundamental to long-term resilience, and in particular a firm's ability to respond to fast-changing situations. In this context, resilience is a valuable asset that should be regarded as a key element of the innovation agenda. Certainly, financial firms that have built strategies and operations around innovation have delivered unique business models to solve problems – challenger banks, lending platforms and payment applications have disrupted the market place and taken a greater market share. Some companies have also embedded resilience into their design.

**“Once you have built resilience in, it’s a heck of a lot cheaper to run. When the technology is there, the dimension you get in real time, saves you money. In this sense, the business case is compelling.”**

Interviewee

There is also a balance between innovation and operational resilience. A new digital channel, for example, will tend to increase operational complexity. A key attribute of firms that successfully balance innovation and resilience is their ability to adapt as systems and business models change.

**“The definition of resilience is expanding with our definition of our services. We are now thinking in terms of customer first rather than from a product lens.”**

Interviewee

Stress and scenario testing are crucial elements of the innovation process, as are methodologies such as site reliability engineering. In all cases, firms must also ensure risk management approaches keep pace with the innovation agenda. Finally, they should reduce complexity when designing and analysing management information. This can also be an effective tool in making sure they focus on the right issues.

## THE AGE OF INNOVATION: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

1. Adapt risk frameworks, governance and strategy to keep pace with the innovation agenda.



### Target:



- Decisions around business models, new products, divestments and M&A will impact future resilience.
  - Firms must consider resilience at every point in the innovation lifecycle, from decision to investment, through design, development and testing and at hand-off into business as usual.
  - As part of any due diligence exercise, firms should assess the operational resilience of the target firm in the same way as they would undertake due diligence of financial and conduct implications.



### RECOMMENDATION

2. Tackle the potential for disruption head on by reviewing the approach to change.



### Target:



- Change management is cited by firms as a key cause of operational incidents and it is an area that firms are able to influence.
  - Firms should consider change methodologies that can support innovation and resilience more effectively, such as removing barriers between the business and IT, or working toward smaller, more frequent releases.
  - Regulators should be mindful of the other regulator-mandated change that needs to be implemented by firms. Flexibility should be afforded to firms by regulators, in the setting and enforcing of deadlines and for process/system implementations which originate with the regulator. This should take account of the impact that multiple regulatory implementations can have on a firm's operational risk profile.



## THE AGE OF INNOVATION: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

3. Routinely address resilience of key services in determining both strategy and investment in systems, including approach to legacy systems.



### Target:



- The current complexity of firms' infrastructure is primarily driven by historic M&A activity where entities have remained on multiple legacy systems.
- Firms should build an understanding of the end-to-end capabilities required to deliver services before making investment decisions on systems.



### RECOMMENDATION

4. Build operational resilience into strategy and business plans, reflecting growth trajectories and systemic importance.



### Target:



- Having a strong, predictable yet proportionate regulatory regime, which allows for innovation, is essential to achieve resilience.
- To address the need for proportionality, regulators should provide a baseline level of expectations and standards, which also take account of global standards.
- Firms should be required to demonstrate how they will improve operational resilience as they grow their customer books and service offerings.
- Regulators should seek information and assurance from firms on how their operational resilience will keep pace with their future growth plans.

# THE ROLE OF GOOD GOVERNANCE

- Firms must break down traditional silos to become more resilient.
- Good quality, future-looking management information is essential - but it is hard to achieve.
- Culture will play a key role in enhancing resilience.

Many UK-based institutions express confidence in their governance frameworks and capabilities. In the FCA's recent technology and cyber resilience survey, for example, some 90% of firms assess themselves as having strong governance.<sup>26</sup> There is some variability with firms subject to the Senior Managers and Certification Regime (SM&CR) - deposit takers, insurers and PRA-investment firms regulated by the FCA and PRA - reporting clearer structures and ownership than others.

The basic rule is that firms have primary responsibility for resisting threats to operational resilience and recovering from incidents. The regulators expect boards to exercise appropriate control. Under the PRA's SM&CR, for example, the Chief Operations Senior Managers Function (SMF) has responsibility for internal operations and technology. To guide firms in their planning, the BoE's Financial Policy Committee (FPC) is working to establish tolerances for the maximum acceptable period of disruption to the delivery of vital business services, for the purposes of stress testing. The time frame is the FPC's 'impact tolerance', which in the regulators' recent discussion paper is a key plank of its proposals for managing operational resilience.

Regulators also continue to promote good governance in their investigations and supervisory rules. In the words of one interviewee who contributed to this report, regulators have "done a good job of raising the profile of governance in recent years".

In November 2018 the Treasury Select Committee launched an inquiry into IT failures in the financial services sector.<sup>27</sup> The Committee will examine the ability of firms to guard against service disruptions and to recover in the event of disruption. The inquiry will explore all aspects of how firms deal with IT failures, including accountability and communication.

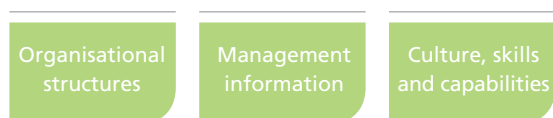
## Defining governance

In our view, governance is the framework of rules, relationships, systems and processes by which a firm is controlled and operates, and the mechanisms by which a firm and its people are held to account. In addition, governance determines the rules and procedures through which a firm's objectives are set and provides the means to deliver strategy and monitor performance. Importantly, it defines where accountability lies and establishes a clear compliance and risk culture.

<sup>26</sup> Financial Conduct Authority, 'Cyber and Technology Resilience: Themes from cross-sector survey 2017-2018', (November 2018), available at: <https://www.fca.org.uk/publications/research/cyber-technology-resilience-themes-cross-sector-survey-2017-18>

<sup>27</sup> Bank of England, 'Record of the Financial Policy Committee Meeting - 26 February 2019', (5 March 2019), available at: <https://www.bankofengland.co.uk/-/media/boe/files/financial-policy-summary-and-record/2019/march-2019.pdf>

For the purposes of operational resilience, it is useful to assess good governance through the following three lenses.



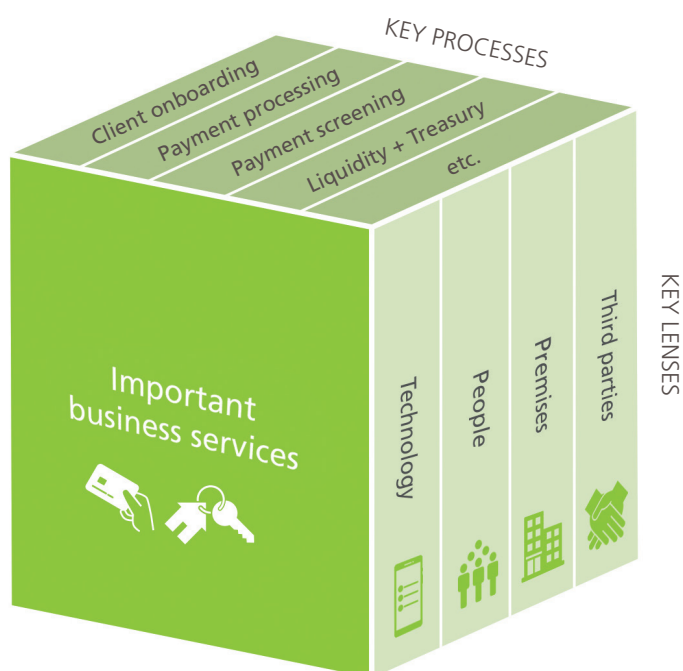
## Organisational structures

Financial firm governance structures are traditionally organised by business line or functional area, albeit with central oversight at board level. The front office and client facing business is generally structured by product or service – an approach that is aligned with the evolving supervisory approach to operational resilience. Other support functions/operations, however, are less well aligned and face more of a challenge.

Operational resilience, in the terms outlined in the BoE, PRA and FCA discussion paper, requires a fundamental shift in perspective and a knitting together of fragmented organisational structures. A key principle of managing that change is leadership. Leaders are required to ensure they have sufficient clarity around how services are delivered. Collectively, there must also be sufficient strategic focus on reporting and decision making to ensure resilience is a functional priority and is practically achievable. Across a diverse and complex organisation this is no mean feat, and it may be that initial steps should be focused on the most critical products and services before being rolled out more widely.

**Figure 7:** A business services approach means cutting across silos

Source: PwC



Rising competition, the growing impact of FinTechs, increased outsourcing and the move towards Open Banking mean financial institutions operate in an increasingly networked and connected environment. Digitalisation, meanwhile, is leading to exponential growth in a number of touchpoints with partners, clients and customers. Against that background, it is incumbent on boards to cast their nets wide in ensuring proper oversight of relevant relationships. They should take a structured approach to identifying and prioritising the firm's most important products, services and assets, using a wider set of considerations than traditional Profit & Loss measurement or compliance.

The PRA's May 2017 supervisory statement defined the Chief Operations Senior Management Function (SMF24) and created a new prescribed responsibility for managing and ensuring the operational continuity and resilience of the internal operations, systems and technology of a firm.<sup>28</sup> The SMF24 role is an exception to the general rule that SMFs cannot be split. In this case, the PRA allows that up to three individuals - including perhaps the Chief Operating Officer (COO) and the Chief Information Security officer (CISO) - may be jointly responsible.

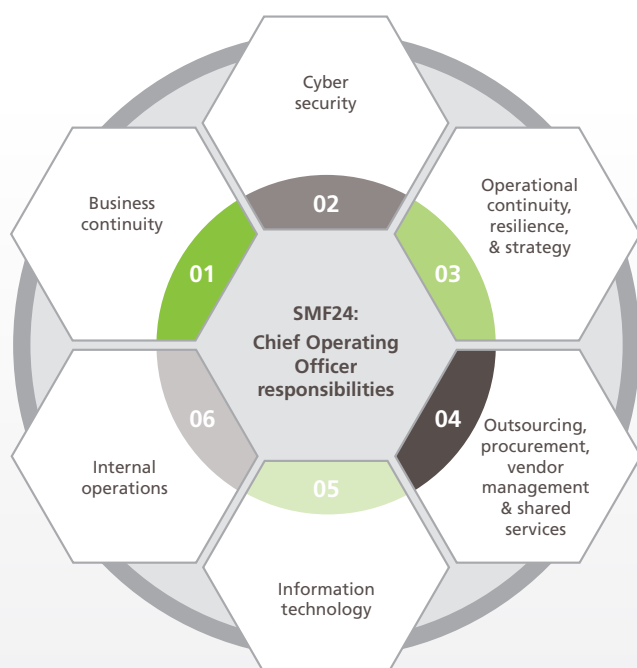
Two dynamics have been identified that will need to be resolved in relation to the SMR. First, SMR responsibilities have been developed based on a 'corporate construct' lens, reflecting a siloed approach, rather than a lens focused on end-to-end business services.

Also, where SMF24 is split, one party inevitably ends up leading the other(s) by way of personal drive or different levels of seniority. This may, for example, catalyse a stronger operational focus if the COO is leading, or a stronger technology approach if the CISO is leading.

28 Prudential Regulation Authority, 'Supervisory Statement 28/15 - Strengthening individual accountability in banking', (July 2018), available at: <https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss>

**Figure 8:** SMF24 has six responsibilities under the SM&CR, covering a multitude of components across a PRA-regulated firm's operating model

Source: PwC



#### Responsibilities map

The SMF24 has six responsibilities set out under SM&CR. The SMF24's responsibilities are far reaching requiring sufficient oversight of the core components of their operating model, such as:

- corporate strategy
- customer offering
- people and process
- information and technology
- organisational structure, roles, networks and governance

An additional complication for some firms is the international context, which introduces complexities into the governance equation and often requires adherence to different local regulations. Positioning operational resilience effectively in an internationally dispersed organisation brings challenges. Smaller UK branches of international parents, for example, are likely to face a battle to exert influence, or encourage a global approach.

**“The UK regulators’ stance has been helpful in allowing us to influence the corporate board.”**

Interviewee

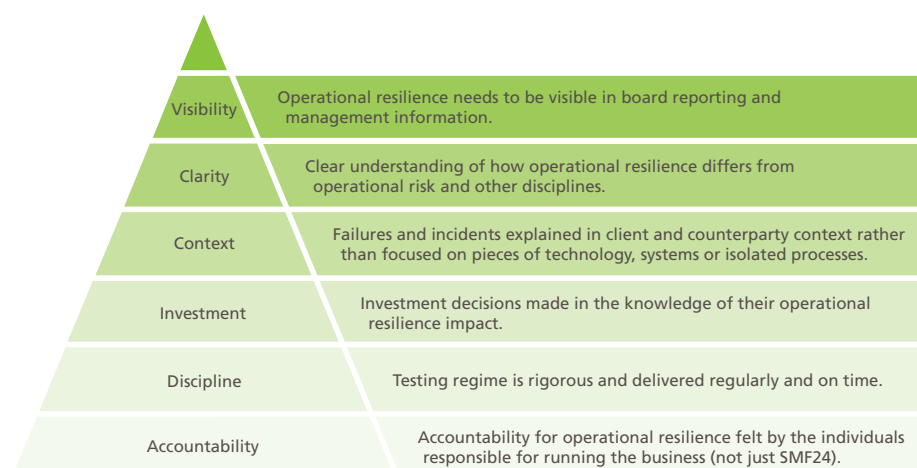
Of course, effective governance structures must not be restricted to senior roles. Instead, they must extend through the firm, and work in both transformative and everyday contexts. This echoes the ways of thinking that have been applied to conduct risk; strong leadership combined with broad implementation at every level.

Still, despite these diverse challenges, some firms are taking action. Several firms have been adapting, flexing and reforming their governance structures to help break down silos and develop an integrated perspective. In addition, some firms have set up operational resilience committees (populated by senior executives and non executives) to drive the agenda and generate traction.



**Figure 9:** An effective governance approach to operational resilience

Source: PwC



## Management information

The challenge for many financial firms is that the quality of information is often poor, or at least insufficient. A common complaint is that feasts, in terms of quantity, are more than offset by famines, in terms of quality.

**“You can have the most perfect governance structures, but they are undermined if the quality of information is poor.”**

Interviewee

In developing their resilience capabilities, firms have a chance to marshal information resources to create a single view that is also aligned with the way that customers perceive them. This in turn will enable a more intuitive appreciation of service delivery and operational performance.

The two key categories of management information relate to risk and performance. Performance information tends to be cast in relation to divisions and business services, aligning it with resilience needs, while risk information is focused on traditional areas of risk, including finance, credit and operations, and is less well aligned.

Operational resilience challenges executives to show they understand the technical detail of delivery of individual services, and their criticality in respect of daily operations and market factors. To achieve this, leaders should resist a siloed approach, and instead seek a more integrated and collaborative representational model through which individual elements are oriented in the context of the bigger picture. With this in mind it may be advisable to seek to access performance, risk and product/service variables on a product/service basis. If this view is aligned with an understanding of the most critical products, services and assets, firms can generate powerful insights to inform governance-related decision making.

The task is complex, and requires firms to make the best use of the tools such as advanced analytics, which can provide a more granular view of the operation of critical business services. Many firms are accumulating skills and capabilities in these areas. Larger firms have an advantage, based on their resources, but none yet have the tools and data quality to do this cost effectively.

In terms of the quality of management information, the optimal approach is forward looking and predictive information that incorporates near misses, echoing the FCA's focus in the area of conduct. Certainly, a mindset of attention to detail (and not disregarding minor events) is likely to be productive in raising red flags and identifying potential threats to operational stability.

**“Never waste the opportunity an event creates.”**

Interviewee

The regulators' discussion paper emphasises the need for firms to develop impact tolerances for disruption to business services. These will certainly be helpful in calibrating information collection and analysis. However, an important precondition is to develop a view of what is 'good' in terms of business service performance. It is important to align tolerance thresholds with those of customers and ensure that this is underpinned by management information and triggers for management intervention.

Getting this right will bring diverse benefits. For example, a key theme in the regulators' discussion paper is around communication. One interviewee talked about the importance of regular communication with customers, and of making sure the firm has something useful to say. “[It is] quite a stressful time when things go down, but we can be more confident with our communications when we know what our tolerances are, as we can be more informed on impacts.”

### Culture, skills and capabilities

The role of governance in defining culture is somewhat complex in the supervisory context. On the one hand, it is a key driver of how a firm is run, and is often an underlying theme of investigations when things go wrong. On the other, it is rarely seen as a critical element of a firm's governance capabilities. Still, there is strong evidence to show that governance can play a key role in culture, which in turn can be an excellent bellweather for operational health. In addition, a positive culture tends to support customer and regulator confidence, and is no doubt correlated with higher levels of trust.

Corporate leaders are increasingly being looked to as governors (focused on 'doing the right thing'), rather than pure commercial managers.

**“A business that loses its trust, loses its business.”**

Interviewee

**“It takes a culture of humility to recognise and deal with your risks - it is the CEO's job to cultivate this culture.”**

Interviewee

Since the financial crisis, regulators and firms have worked to build trust, initially in terms of prudential soundness and good conduct. It now falls on the financial services sector to deliver trust in terms of security, robust operational delivery and availability, all of which are a significant ask.

Certainly, senior management is required to set the tone, ask the right questions and seek the right information. This is the best way to integrate operational resilience. In addition, a healthy reciprocal relationship with leadership is required. People must be trusted to provide the right information to allow senior management to make decisions and to flag where things go wrong. In this context, senior managers are required to take a lead in promoting transparency and openness.

Culture is highly correlated with talent, and it may be that the market currently lacks sufficient talent to deliver the strategic approach required, with these skills being in high demand and expensive. Firms may need to look beyond financial services to find talent with the right skill set to support resilience. It will take time and experience of operational incidents for a resilience culture to mature to drive optimal models and approaches.

## THE ROLE OF GOOD GOVERNANCE: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

5. Develop a clear view of a firm's purpose and place in the context of the wider economy when establishing governance arrangements.



Target:



- To be able to drive resilience effectively in their most critical business services, firms need a clearer view of their purpose in the context of the wider economy. For many retail-focused businesses this will be clear.
  - Some wholesale businesses may need to carry out analysis to identify how their products and services support the wider economy (e.g. where a cash flow product provides downstream liquidity for a SME to fund a month's payroll).
  - Firms should collaborate by sub-sector to identify important business services, potentially harmonising taxonomies where possible. This will provide benefits in relation to stress tests and tolerances by creating industry standard views of business services.



### RECOMMENDATION

6. Establish individual accountability and collective responsibility to better support resilience decision making by extending existing regulatory tools and governance structures.



Target:



- Resilience is a collective commercial imperative that should be considered by all.
  - Firms should consider the potentially negative implications of splitting the SMF24 role where this dilutes accountability.
  - Firms should use SMR to hold a broader range of senior individuals to account for operational resilience. In particular SMF6s (head of key business area function) should be responsible for embedding operational resilience into their business areas, with individuals taking responsibility for each end-to-end process. These individuals should be mandated to work across silos where they exist.
  - Firms should also take operational resilience into account when assessing the fitness and propriety of individuals captured by the certification regime.
  - The SMR regime should be extended to FMIs to reflect the importance of resilience in relation to their offering.

## THE ROLE OF GOOD GOVERNANCE: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS

- Leaders should consider the maturity of their approaches and their capabilities, making sure that SMF24 has a seat at the senior table and is truly accountable for decision making.
- Firms should consider how the recommendations set out in TheCityUK's and Marsh governance report<sup>29</sup> could be expanded to cover wider operational resilience.



### RECOMMENDATION

7. Establish comprehensive end-to-end management information and reporting for important business services.



#### Target:



- Regulators are looking to treat operational resilience on a par with financial resilience, and boards need to ensure their firms have robust governance arrangements in place to manage operational resilience.
- Management teams should review and redesign management information to ensure it is meaningful and predictive. This will require breaking down silos and pivoting from current piecemeal reporting (e.g. cyber, business continuity planning/disaster recovery testing, service level agreements and incidents) to an end-to-end business service view.



### RECOMMENDATION

8. Encompass operational resilience skills and capabilities in management development programmes.



#### Target:



- The skills and capabilities required to support resilience are scarce and complex, particularly as delivery models and products and services are being transformed by new technologies.
- Firms should look outside financial services to secure the best talent.
- They should develop talent attraction and retention, and management development strategies to increase resources and improve understanding of operational resilience among senior management.

<sup>29</sup> TheCityUK - Marsh, 'Governing cyber risk: a guide for company boards', (April 2018), available at: <https://www.thecityuk.com/research/governing-cyber-risk/>

## THE ROLE OF GOOD GOVERNANCE: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

9. Be more transparent about the threats to the ongoing delivery of important business services through more detailed external disclosures and regulatory reporting.



### Target:



- Risks to the ongoing delivery of key services should form a part of shareholders' overall view of a firm.
  - Firms should consider what disclosures they could/should be making in relation to resilience or risk of failures, for example, covering material risks, the measures used to manage those and oversight/investment governance. These could be through Internal Capital Adequacy Assessment Process (ICAAPs), Own Risk Self-Assessment (ORSAs), annual reports or through other means.
  - Firms should consider the benefits of developing industry-recognised standards or certifications to provide assurance to shareholders, regulators and customers.
  - Regulators should review recent improvements in reporting (e.g. via the EU's Payment Services Directive 2) and consider where further standardisation would improve stakeholders' ability to differentiate firm resilience.
  - Firms should adopt the recommendations outlined by the Task Force on Climate-related Financial Disclosures (TCFD) in June 2017, in their approach to disclosing the risks to operational resilience.



# REGULATION AND SUPERVISION: A SHIFTING LANDSCAPE

- Resilience is first and foremost a business imperative, but there is a role for regulation.
- Proportionality is key to supporting both resilience and innovation.
- You are only as strong as your weakest link in a global financial ecosystem. Resilience must be predicated on international consistency and cooperation.

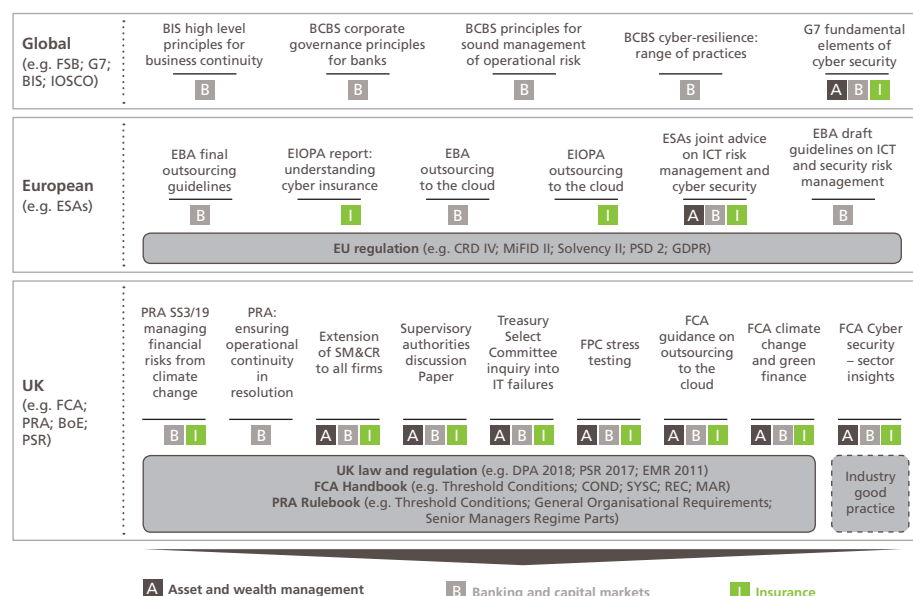
Operational resilience has risen to the top of the regulatory agenda over recent years, due both to an increase in threats and the potential impact on customers and the financial system. The issue falls under the remit of a cross section of regulators and policymakers, including HM Treasury, the Bank of England's Financial Policy Committee, the PRA, the FCA, and the Payments Systems Regulator (PSR). These individually, and jointly, have acted to boost awareness and encourage firms to act.

The recent intensification of regulatory focus builds on established regulation relating to operational resilience, including outsourcing, business continuity planning and operational risk management. For example, the European Banking Authority (EBA) Draft Guidelines on Information Communications Technology (ICT) and Security Risk management, and the FCA guidance on firms outsourcing to the cloud and other third-party IT services.<sup>30, 31</sup>

**Figure 10:** Illustration of volume of regulatory thinking shaping the operational resilience agenda

Source: PwC

**Note:** Financial Market Infrastructures (FMIs) are excluded from the chart. There are general principles for FMIs published by IOSCO/CPSS (2012) and some specific guidance on cyber resilience (2016)



30 European Banking Authority/CP/2018/15, (December 2018), available at: <https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management>

31 Financial Conduct Authority, 'FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services', (July 2018), available at: <https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it>

The PRA in 2017 took a significant step forward with the addition of the SMF24 to the SM&CR. At relevant firms the SMF24 has responsibility for operations and technology. In conducting interviews for this report, TheCityUK and PwC were struck by the number of executives that emphasised how the introduction of SMF24, and SM&CR more generally, had helped crystallise focus and move the operational resilience topic from the second to the first line of defence.

In addition, there are a number of relevant international standards. The International Organization for Standardization (ISO) in 2017 published ISO 22316 in relation to security and resilience. The standard defines resilience as “the ability of an organisation to absorb and adapt in a changing environment” and provides guidance on principles around areas including culture and risk management. CPMI-IOSCO published guidance on cyber resilience for financial market infrastructures – one of a large number of global, regional and national policies, statements and guidelines on the cyber issue.<sup>32</sup>

While the broad regulatory focus on operational resilience is constructive, it also carries some risk. One in particular is that a range of regulatory initiatives creates a confusing mix of overlapping requirements. In the worst case it may undermine the resilience it is intended to create. The BoE, PRA, FCA discussion paper represents a partial antidote. The discussion paper is the first policy document to present an overarching framework that brings together historical and current thinking on best practice.

---

<sup>32</sup> The Committee on Payments and Market Infrastructures (CPMI)1 and the Board of the International Organization of Securities Commissions (IOSCO), ‘Guidance on cyber resilience for financial market infrastructures’, (June 2016), available at: [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

## The BoE/PRA/FCA discussion paper

### Building the UK financial sector's operational resilience

The joint paper sets out a framework for improving the operational resilience of financial institutions and financial market infrastructures in the UK. It signals an expectation that the industry should accelerate efforts to boost resilience to a range of risks. Key recommendations include the following:

- Firms should establish impact tolerances for disruption to the provision of important business functions (e.g. lending, trading of financial instruments, providing insurance contracts). The tolerances could include maximum duration of disruption, volume or number of customers affected.
- When setting impact tolerances, firms should prioritise business services that have the potential to threaten viability, cause harm to customers and market participants or impact financial stability.
- Impact tolerances should be captured in an impact tolerance statement. Regulators may choose to set their own impact tolerances if they are not satisfied with those set by the firms themselves.
- Operational resilience can be best addressed by a focus on business services and understanding the systems and processes required to support these (including those provided by third parties or other entities in the same group).
- Governance and individual accountability will continue to be a key focus. Boards and senior management should be fully engaged in improving operational resilience, and the regulators will continue to focus on individual accountability through the Senior Managers Regime.

The proposals recognise that direct regulation will not be the primary driver of operational resilience. In the regulators' view it strikes the right balance between prescription and guidance. In particular, it recognises that the primary responsibility for ensuring operational resilience rests with firms and their boards. As part of that responsibility, boards should consider operational resilience in the context of their wider strategies and consider holding themselves to higher standards as the business grows.

The regulators will assess firms' ability to meet their stated impact tolerances and more generally enhance overall operational resilience as part of ongoing supervision. To encourage consistency, the regulators may provide guidance on metrics that firms should use when assessing their ability to meet impact tolerances.

In defining and discussing operational resilience, the regulators' discussion paper has helped solidify the concept in the minds of industry leaders. One interviewee said, "It is easier to have it as an agenda item now it has a name. This explicitness is important as financial services evolves and we need to be increasingly cognisant of operational resilience". This is particularly important in a dynamic technological and regulatory environment, in which many firms are implementing significant change in core systems and business models. However, by the nature of the subject matter, the construction of a sound framework will be iterative and will take time. It involves a cultural shift for firms, and a change in approach for regulators.

PwC's work with other sectors has shown that regulation is not necessarily by itself a driver of operational resilience. There is a risk that firms can be distracted from the business imperatives of resilience in favour of satisfying the regulators. We see good levels of resilience at firms that are culturally comfortable with the notion that things will go wrong and it is their responsibility to ensure that this doesn't result in disruption to business services.

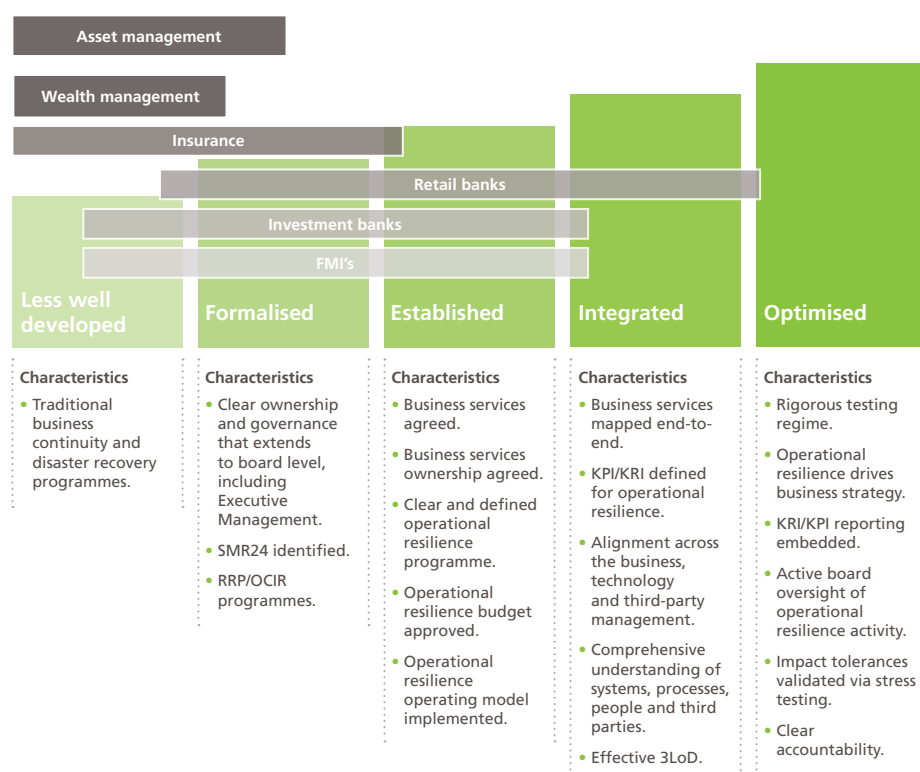
## A flexible, judgement-led approach

The nature of operational resilience means that prescription is generally not appropriate. Since operational resilience is an 'outcome' that can be achieved in a number of ways, one size does not fit all. Indeed, industry participants are at varying stages of development of resilience strategy and implementation. Proportionality is essential, given the proposals which apply to all firms, whatever the size.

**Figure 11:** High-level assessment of firms' levels of maturity of their operational resilience

Source: PwC

**Note:** This is subjective and based on PwC's experience of working with clients on a variety of projects and over a period of time



Regulation in this context should set a baseline level of expectations and standards. However, in almost all cases, firms should seek a higher standard for themselves and their customers. One reason is that, in an increasingly competitive environment, robust operational resilience can be a key differentiator.

UK regulators are rightly considered to be among the most advanced when it comes to operational resilience. However, resilience straddles different aspects of the current UK framework. In the first instance, operational outages can harm consumers, meaning it is an FCA concern. If an incident impacts on a firm's safety and soundness, by contrast, it would fall under either the FCA, PRA or BoE, according to the types of firm which they prudentially supervise. The FPC would become more involved where there was a systemic implication. The implication of this structure is the potential for differing levels of involvement – the FCA's tolerance for disruption, for example, may be less than that of the PRA or BoE.

The operational resilience agenda will require a change in supervisory approach and a deep understanding of business drivers, strategies, operating models and culture. For example, the regulators have started to take a more holistic approach to decisions involving proposed M&A activity, including considering the impact on operational resilience, but there remains a lack of internal guidance for supervisors on how they should approach this.<sup>33</sup> With that in mind, regulators may need to consider whether they require more resources and subject matter experts, enhanced through secondments from the private sector where appropriate, or senior advisors with relevant expertise.

### The importance of coordination

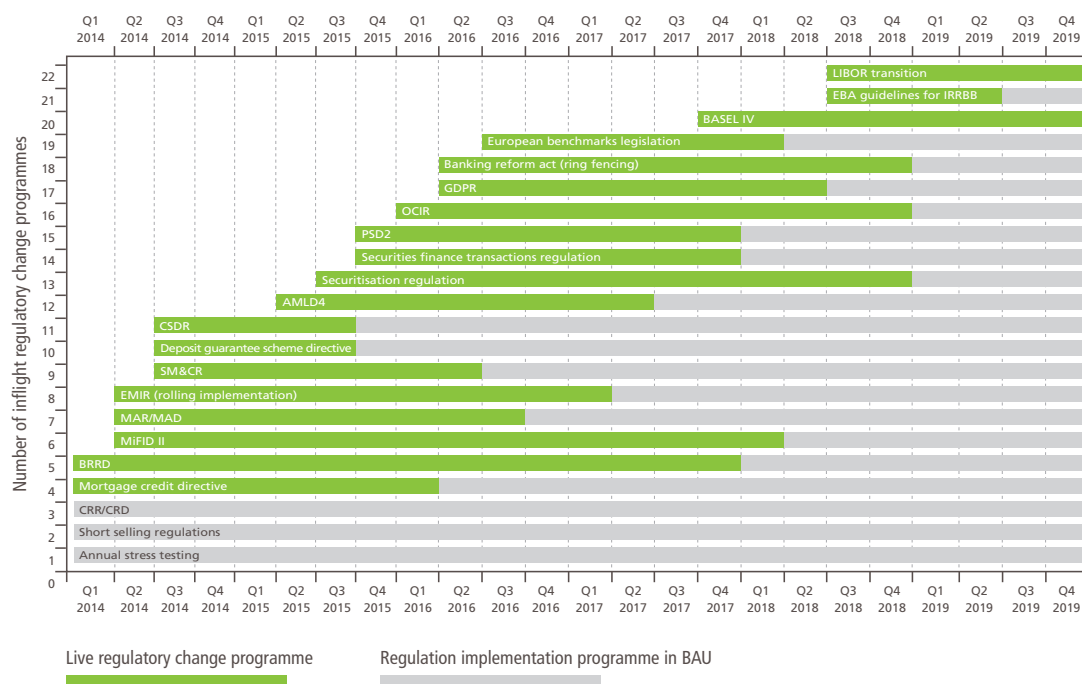
Post-crisis regulation has driven numerous shifts in financial industry structures, organisational set ups and business models. Often these require significant investment in IT infrastructure and data capabilities to support reporting requirements, risk management, finance and customer facing activities. A large financial institution may have hundreds, if not thousands, of change programmes running concurrently. The operational and financial impacts of these are considerable, often requiring a significant amount of resource and attention from senior leadership.

In addition, there is no clear mechanism for coordinating the implementation of new requirements or to prevent firms from being overburdened with condensed implementation dates. In future, UK regulators may wish to mitigate the impact of extensive regulatory change and its threat to resilience.

### Summary of regulatory initiatives by sector

**Figure 12:** Banking regulatory change requirements

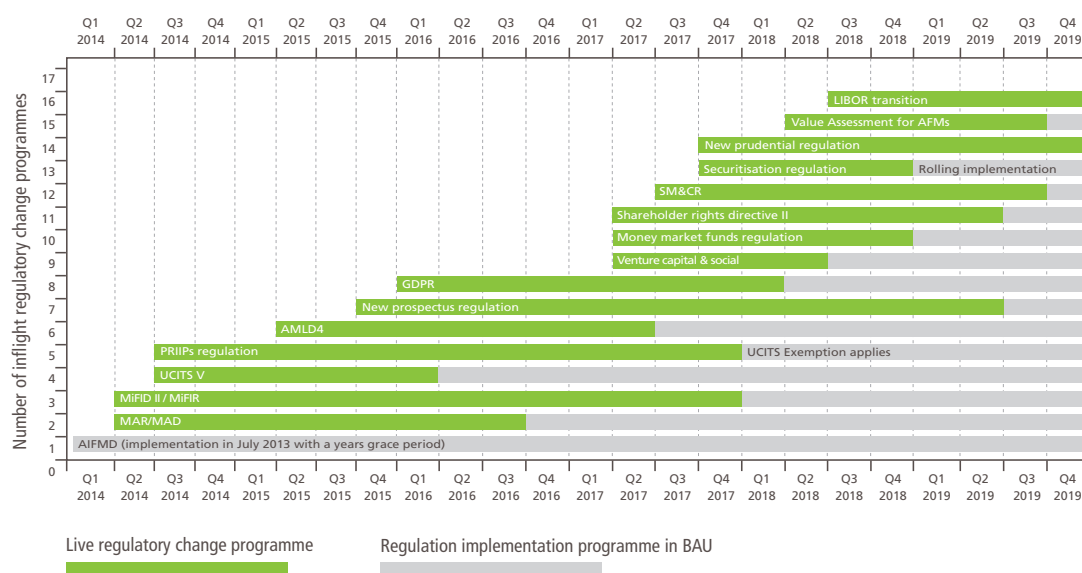
Source: PwC



<sup>33</sup> Bank of England, 'Independent review of the supervision of the Co-operative (Co-op) bank', (March 2019), available at: <https://www.bankofengland.co.uk/news/2019/march/independent-review-of-the-supervision-of-the-co-op-bank-published>

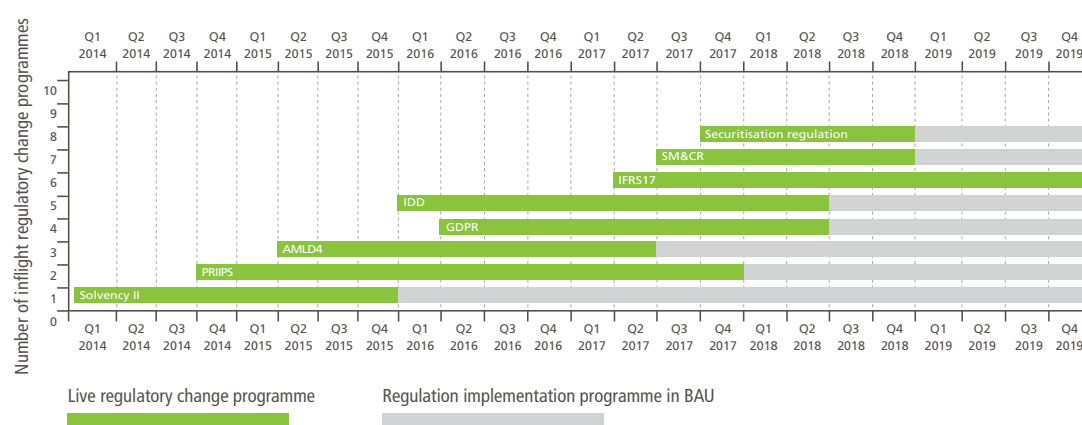
**Figure 13:** Asset & wealth management regulatory change requirements

Source: PwC



**Figure 14:** Insurance regulatory change requirements

Source: PwC



Operational resilience covers many different areas of existing regulatory focus, including OCIR, solvent wind-down, cyber security, third-party operational risk and reporting, complaints, and financial crime. In this context, TheCityUK and PwC welcome the review of existing regulation signalled in the discussion paper.<sup>34</sup>

<sup>34</sup> Bank of England, Prudential Regulation Authority, Financial Conduct Authority, 'Building the UK financial Sector's Operational Resilience', Discussion Paper, (July 2018), available at: <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>

## International consistency and cooperation can help

UK regulators are taking a lead on operational resilience. However, as with all regulation, standards will be most effective if applied globally. Currently, there is little standardisation across countries, and certainly less than there is for financial resilience (for example, through the Basel Accords).

While there are potential benefits from taking the lead, it also brings risks and potential costs should international standards eventually conflict. The Basel Committee on Banking Supervision (BCBS) has announced that in 2019 it will examine risks from emerging technology and the impact on regulatory and supervisory strategies. The BCBS will also publish updated guidance and a survey on supervisory metrics for measuring operational resilience. At this stage, other standard setters such as the FSB, IAIS, IOSCO, and CPMI have not announced similar initiatives.

The UK's financial services sector is perhaps the most globalised in the world. Most of the largest firms have operations in multiple jurisdictions. This brings significant cross-border dependencies, which can improve operational resilience. For example, during the terror attacks on September 11 in 2001, a number of global investment banks were able to continue operating because of interoperability between New York and London. Still, the globalised nature of the industry means that coordination, cooperation and indeed trust among regulators is vital. In some cases that may mean overcoming challenges around practice and culture. It is unclear, for example, how the UK's outcomes-based regime would translate in a more prescriptive environment. With a number of global firms headquartered in London, there is an extra-territoriality implication for UK regulators to consider. This provides a great opportunity for consistency, but also comes with responsibility when considering various approaches.



## REGULATION AND SUPERVISION: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

**10. Continue to take a lead role in driving consistent global regulatory standards.**



### Target:



- Fragmented and inconsistent regulatory and supervisory approaches across the world are problematic for UK financial stability and the sector. Driving international consistency also reduces the cost of regulatory compliance for UK-based firms doing business internationally.
  - As a 'first mover', the UK authorities should seek to drive progress in designing internationally consistent standards for operational resilience in the FSB and other standard setters such as the BCBS and IOSCO.
  - The BoE and the FCA should ensure they commit adequate regulatory resources to influencing international standards, sharing learnings and providing access to tools and approaches being used and developed.



### RECOMMENDATION

**11. Provide greater clarity to firms on how to govern and manage operational resilience where there are already existing initiatives that overlap.**



### Target:



- There are existing and potentially overlapping regulatory initiatives that support operational resilience.
  - Regulators should review and assess the effectiveness of existing initiatives before introducing new ones.
  - Firms should leverage their work in respect of OCIR, recovery and resolution planning (RRP), cyber resilience, and ICT to support operational resilience.
  - Regulators should provide more guidance on how these regulatory initiatives should interact.
  - Regulators should have operational resilience in mind when considering the cost/benefit and timing of regulatory change.
  - They should consider how they can adapt and enhance existing mechanisms to support operational resilience, rather than introduce new ones. For example, the current Supervisory Regulatory Evaluation Process (SREP) for banks could be adapted. The findings from S.166 reviews and publication of more detailed Final Notices could be used for root cause analysis across sectors.

## REGULATION AND SUPERVISION: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

12. Enhance supervisory capabilities by expanding skills and experience.



### Target:



- Skills and experience should be assessed based on the ability to support both resilience and innovation across the financial services sector.
  - The PRA/FCA should consider recruiting more senior advisors with a background in technology and other operational resilience disciplines to help support supervisory teams and interface with regulated firms on a proactive basis.
  - Regulators should consider other skills and experience, including individuals from an operational background, as part of their recruitment and secondment arrangements, to develop expertise in operational resilience.

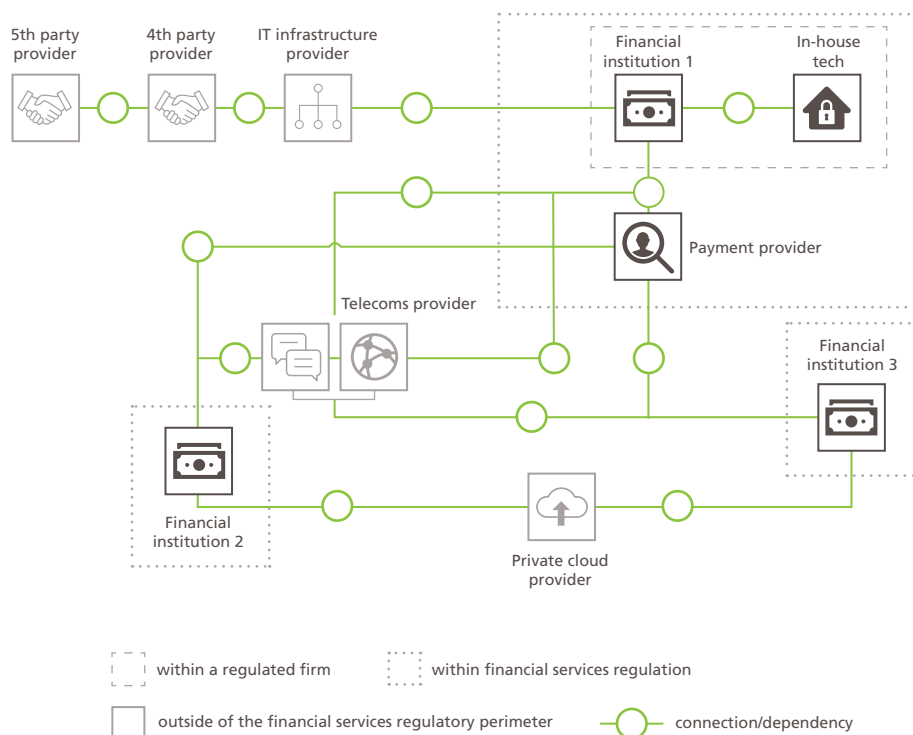
# A CONNECTED WORLD: SYSTEMIC IMPLICATIONS

- As cross-sectoral dependencies grow, the resilience of individual participants cannot be viewed in isolation.
- Cross-sector collaboration improves understanding and enables more informed planning, both for individual firms and collectively.
- Sharing cultures and goals with third-party providers will support resilience.
- Services are increasingly provided from outside the regulatory perimeter. Is it time to redraw the boundaries?

As global financial services embrace digitalisation, they are becoming more connected and interdependent. The impact of proliferating digital touchpoints and multiple data resources is to create an intensely networked environment, in which every firm is reliant on numerous other participants to operate and serve customers. The emergence of several thousand FinTechs and growth of API-enabled ecosystems, in which connected businesses share resources, has accentuated the trend and deepened links between financial companies and the wider economy. As dependencies grow, the resilience of individual participants is increasingly dependent on the resilience of others. Indeed, the resilience of the financial system as a whole depends on the connections among individual participants.

**Figure 15:** Financial services ecosystem dependency map

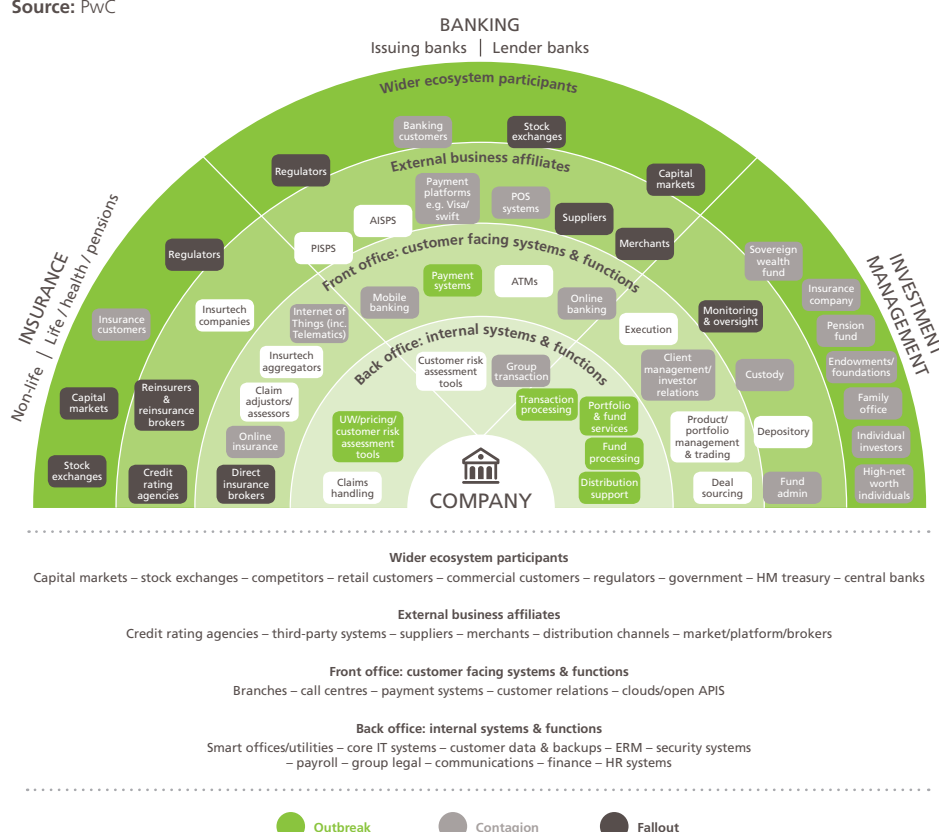
Source: PwC



Scenarios are a powerful way of assessing and communicating the operational resilience of an ecosystem. The figure below shows how a highly contagious malware can spread through the financial services sector services and organisations, as a result of shared IT systems and operations. The footprint of operational disruption increases through the various stages of the attack: outbreak, contagion and fallout.

**Figure 16:** An example of how an event could have systemic effects

Source: PwC



Growing connectedness is the result of increasingly digital operations, but also new ways of working. The trend toward outsourcing is a contributing factor, while moves to mutualise risk, for example through central clearing of derivatives, has a centralising effect. The connectedness of global networks, meanwhile, increases contagion risk, with threats such as cyber attacks much more susceptible to spreading at speed. In short, technological innovation is a source of both operational efficiency and operational risk.

In a dynamic environment, common standards can bring significant benefits. For example, impact tolerances for a particular business service can be applied across jurisdictions, meaning resilience can become location agnostic. Firms should take an outward view of their services and impacts, as well as their dependence on participants, disruptions and behaviours. They should work with partners as far as possible to seek standardised solutions.

There are four key areas of focus listed below.



## Cross-sector collaboration and testing

The financial sector works collaboratively as a matter of course. However, it requires common response mechanisms and standardised playbooks to enable speedier stabilisation of volatile situations.

In some areas, these kinds of collaborative initiatives are starting to be put in place and could potentially be expanded to cover wider operational resilience. The Cyber Security Information Partnership (CSIP), for example, is a joint industry and government initiative set up to exchange cyber threat information in real time. The partnership aims to provide a secure, confidential and dynamic framework that increases situational awareness and may reduce the impact of cyber attacks. In the US, Sheltered Harbor is a collaborative financial services organisation that offers a data vault for institutions to backup critical data offline. It also offers a resiliency plan (comprising business and technical processes and key decision protocols to be activated in the case of an event) and certification to show participants have reached a specified standard of resilience. Sheltered Harbor is a not-for-profit organisation with an independent board of directors made up of participating financial services firms. In the UK for example, the Financial Sector Cyber Collaboration Centre, offers an operational solution to these issues through industry and regulatory cooperation.

The challenge for UK financial market participants is to develop security systems and at the same time manage potential concerns over data privacy. Companies must be willing to share experiences and expertise and participate in cross-sector testing of plausible scenarios. This can improve understanding and enable more informed planning and preparedness, both individually and collectively. Modelling of participant and consumer behaviour is recommended. In addition, it may be that the UK government can play a role in convening and facilitating private and secure communication channels.

## Substitutability

Substitutability is the ability of a system, device or process to operate instead of another system, device or process, and is therefore an important capability in terms of sustaining resilient operations. However, complex and bespoke processes and technology severely restrain the ability of firms to substitute.

The response to poor substitutability is standardisation and simplification, which are key enablers of so-called resilience by design. By virtue of digitalisation, many financial firms are embracing standardisation, for example in relation to data, which enables simpler and more streamlined decision making. By extension, there is no reason why standardisation should not extend across the industry, which would naturally contribute to common approaches and greater substitutability. Of course, the flipside is that standardisation may erode competitive advantage.

In areas such as payments, substitutability needs to be agreed by participants and providers to be effective. All participants should know when to substitute, and to which service. Viability and robustness must be established through shared testing. As business models change, new market entrants may proliferate leading to the need to adapt service delivery mechanisms. A move towards substitutability may encourage a more agile approach, which in turn may lead to simplified services and increased multi-source delivery.

The concept of substitutability may also be applied to third-party relationships and procurement. Firms may opt to retain a primary supplier but also to sustain relationships with secondary and tertiary suppliers so they can substitute as seamlessly as possible should the primary relationship fail. A related strategy may be to split providers across production and backup services so that firms can access backup data to allow them to recover more easily and/or find an alternative supplier. A useful approach may be a supplier symposium to educate on regulatory requirements and needs.

Recent technology advances in cloud services have the potential to allow application owners to cherry pick venues, choose multiple venues or pick the most optimal venue based on availability, cost and security. Tools are emerging to help. However, these solutions are not fully proven and there are also cost and performance implications associated with managing applications across multiple cloud providers and the movement of data. Firms should actively monitor developments and embrace opportunities to test technology as a basis for substitution.

Another approach to substitutability could be the establishment of a skeleton 'cold' site for deployment at short notice in the event of an incident. However, the cost associated with maintaining such a facility, together with the operational risk arising from relying on an unused and untested solution, would have to be weighed carefully. Also, firms must be prepared for significant operational risks involved in deploying an unused/untested facility at short notice.

In conclusion, substitutability can be a useful strategic and tactical tool to enable operational resilience. However, to optimise its impact, firms (and perhaps also regulators) should be as clear as possible in defining appropriate use cases. It is impractical to expect wholesale substitutability. Equally, it is important to recognise dependencies that are not suitable for substitution.

**“If this goes down, we have a big problem, but it’s unrealistic to have a Plan B.”**

Interviewee

For these types of dependencies, it may be necessary to apply additional protection. To achieve this, firms will need to reclassify their outsourcing/third-party dependencies. These may comprise the following:

- **Essential large-scale outsource providers.** Applies where firms are service takers and where the services are mainly managed through contracts. These are likely to provide the same or similar services to numerous market participants (e.g. cloud platforms). In this case, groups of firms may arrange a pooled audit, which may take the form of an ISAE 3402-style certification focused on resilience rather than controls.<sup>35</sup> The contractual arrangements with these providers will also be essential to support resilience, with, for example, greater focus on the exit process, data transfer and multi-region backup.

<sup>35</sup> International Standard on Assurance Engagements (ISAE) No. 3402, 'Assurance reports on controls at a service organization', (June 2015), available at: <http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isa-3402.pdf>

- **Smaller service providers that deliver specific services.** Some of these may be suitable for substitutability, but pooled audits and contractual arrangements will also be important.
- **Systemically important providers.** For these providers, a Plan B is unrealistic. Industry and regulators need to think of alternative ways to manage resilience. As well as pooled audits, and participation in stress-testing exercises, regulators may also wish to consider reassessing the regulatory perimeter.

One tried and tested approach when technology fails is to revert to manual processes. In sectors such as insurance, where there may be an issue with existence of cover, this can be provided without the need to see the actual transaction and can be conducted on paper. In the London market much is still done with paper signatures (although these are likely to disappear in the next few years as digital signatures take over).

The ongoing automation of the financial services sector may ironically increase operational risk, because it will remove many of the manual work-arounds that currently provide a safety net.

## Suppliers and service providers

Third-party service providers are a significant source of connectedness. From payments service providers, to central clearing counterparties (CCPs), FinTechs, as-a-service companies, and utilities in areas such as on-boarding and asset servicing, firms are increasingly linked. Resilience is only as strong as the weakest link, and for many firms, supply chain and upstream are a primary source of risk. In addition, companies realise that their vulnerability is not only their vendors (including fourth and fifth parties) but also those connected to them, including their customers. Finally, many providers do not offer structured assurance to their client bases.

As a first step, firms need to analyse potential risks associated with suppliers, which may be exacerbated by concentration risk. It may be that firms are best served by bringing firms in, rather than keeping them at arm's length.

**“We require more from our vendors – we require them to be a partner more than a supplier.”**

Interviewee

A sense of mutual resilience can be reinforced through common goals, with a shared mission likely to be as, or perhaps more, important than contracts and audit rights. Some firms have established joint operating committees for critical suppliers, which act as a clearing mechanism at CEO level and ensure there are no line management standoffs.

There is a question as to the role of regulators in respect of large, systemically important suppliers, some of which are bigger than their clients. In some senses, the financial services sector has become a net ‘service taker’. Several of these monopoly/oligopoly providers, for example, in cloud services and data, are embedded in the infrastructure of the sector. However, currently there is a very real legal and regulatory lag in supply chains. There may be merit in regulatory guidance to drive new contract terms, particularly where substitutability is limited.



Of course, size is not everything. Smaller suppliers may be just as important as large providers. Criticality it should be measured based on the business services supported, rather than the scale or market value. In fact, it is often niche or more traditional suppliers that present the greatest threat to operational resilience. There was an acknowledgement among a number of interviewees that there was a role for them to educate their suppliers through audit activities and feedback.

One conundrum facing the industry is how far down the supply chain they should look in respect of oversight. It makes sense to keep an eye on primary suppliers, but what about their suppliers, and the suppliers of their suppliers? Clearly, there are significant challenges the further removed a company is. Some firms routinely request veto or permission rights on arm's length suppliers, but this is often resisted by companies further up the supply chain. As a result, the issue remains an inherent tension.

From a geographic perspective, a firm's responsibility for suppliers is envisaged in the regulators' discussion paper as being relatively extensive. Once impact tolerances are set, for example, they will be relevant to the systems and processes supporting business services wherever they are located. This includes the systems and processes of outsourced service providers, the regulators' discussion paper<sup>36</sup> said. This might require consideration of the extent to which standards differ among jurisdictions. In general, the impact tolerance for a particular business service would need to be met regardless of the location of supporting systems and processes.

Audit rights are already widely used, but good practice requires firms to change the substance/proximity of their relationships with critical suppliers to extend to joint operating committees, staff physically sitting in with key vendors, greater substance to and frequency of audits, and more regular supplier symposiums.

## Operating models and concentration risk

The pursuit of resilience is in fact one of the strongest arguments for centralisation. CCPs, for instance, were promoted following the financial crisis to reduce counterparty credit risk on derivative transactions. However, concentration risk is the other side of the mutualisation coin. With all over-the-counter (OTC) derivative trades cleared through just a few CCPs, the failure of a single CCP would have significant operational consequences. CCPs are well set up for financial resilience, employing a waterfall of internal and member liabilities, but there is no equivalent operational mechanism.

Regulators are better placed than individual firms to see the cumulative impact of concentration risk. Arguably, firms have a responsibility to undertake effective due diligence and take steps to avoid concentration risk when identified. Still, concentration risk can accumulate quite quickly, particularly where new entrants find a compelling solution that is quickly adopted by a number of participants. In these circumstances, the vendor in question may also become overstretched.

<sup>36</sup> Bank of England, Prudential Regulation Authority, Financial Conduct Authority, 'Building the UK financial Sector's Operational Resilience', Discussion Paper, (July 2018), available at: <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>

## A CONNECTED WORLD: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

13. Find collective solutions to common challenges by establishing cross-sector initiatives around scenario testing, stress testing and information sharing.



#### Target:



- To stifle the exploitation of current vulnerabilities and stay ahead of emerging threats, firms must be willing to share experiences and participate in multi-firm scenario testing.
- The regulators should establish an effective information sharing group to participate in coordinated cross-sector stress testing for operational resilience.<sup>37</sup>



### RECOMMENDATION

14. Address the potential for 'firm paralysis' by integrating recovery and resolution and cyber arrangements across the sector.



#### Target:



- Without careful planning, options for dealing with an event that causes firm paralysis are limited.
- Firms need to stress test a range of scenarios including a prolonged or terminal outage.
- Contingency plans for such an event should include coordination with other industry participants to support the ongoing delivery of important business services and positive outcomes for customers.

<sup>37</sup> Examples include: Cyber Security Information Sharing Partnership (CISP), Bank of England's Cross Market Operational Resilience Group (CMORG), Securities Industry Business Continuity Management Group (SIBCMG), FCA Cyber Coordination Groups

## A CONNECTED WORLD: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

**15. Map the sector and its dependencies to understand systemic operational interdependencies. This could include reconsidering the regulatory perimeter.**



Target:



- A central view of dependencies is needed for regulators to assess the cumulative impact of concentration risk across sectors and consider the regulatory perimeter. This exercise would also help make operational resilience stress testing more effective.
  - In order to proactively monitor concentration risk, regulators should require firms to extend their registers reflecting arrangements with third parties (including outsourcers) to include all arrangements that support important business services.
  - Regulators need to understand and map operational dependencies, including reliance inside and outside the regulatory perimeter.
  - Sector mapping should be employed to identify concentrations of supply and any need for active participation of non-regulated firms in market testing and stress/reverse - stress testing.
  - Policymakers should consider whether regulators have the powers they need where risks are outside their current remit.
  - Regulators should align the definition of material outsourcing and FCA General Guidance on Outsourcing (SYSC8) guidance to third-party activities that support important business services across sectors.



### RECOMMENDATION

**16. Work with technology and other providers to develop standardised support frameworks and opportunities for substitutability of key infrastructure services.**



Target:



- With many firms now outsourcing key parts of their infrastructure, there is an opportunity to standardise some of these 'utilities' and therefore improve the substitutability of key services. Regulators should:
  - use their convening powers to encourage the development and adoption of utility solutions.
  - work with global counterparts to ensure regulatory alignment of shared platforms to allow for interoperability across geographies and locations.<sup>38</sup>
  - enhance common standards of service for critical and common third parties.

<sup>38</sup> TheCityUK, Deloitte & Santander, 'Splitting the Bill: The role of shared platforms in financial services regulation', (November 2018), available at: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-the-cityuk-splitting-the-bill-the-role-for-shared-platforms-in-financial-services-regulation.pdf>

## A CONNECTED WORLD: RECOMMENDATIONS

The following recommendations are targeted towards industry and/or regulators



INDUSTRY



REGULATORS



### RECOMMENDATION

**17. Overhaul supplier management frameworks to improve operation of key third-party provided services.**



Target:



- With the delivery of important business services increasingly reliant on third-party firms, there is a need for a concerted effort to improve the way in which these key relationships are managed as partnerships.
  - Regulators should provide further guidance on expectations for contractual arrangements with service providers.
  - Firms should review contracts to consider how to better align their interests with key suppliers through, for example, the development of common goals and joint operating committees and alignment by operational resilience outcomes.
  - The industry should enhance audit rights to provide greater proximity and access. It should also extend the use of pooled audits where service providers offer the same or very similar services to a number of market participants. These audits should focus on resilience rather than simply on controls.
  - Firms should require suppliers to support scenario stress tests.

# CONCLUSION

The financial services sector is rapidly changing, with digitalisation, regulation and shifting customer needs requiring a new generation of operating models. Change brings significant opportunity, but also unintended consequences, including risk in the change process itself, cybercrime, and rising interconnectedness that carries echoes of the 2008 financial crisis. To date, efforts to offset these threats have been less than sufficient. The result is a rising chance of interruption to vital business services and, in the worst case, a damaging systemic meltdown.

Financial services firms and regulators are well placed to boost operational resilience and support business as usual delivery of services in the face of operational difficulties. The positive outcomes of doing so are significant. They include more sustainable performance, leadership in the global context and a boost to the confidence, reputation and investability of UK financial services.

By working collaboratively with regulators and wider stakeholders, the financial and related professional services ecosystem can take forward the recommendations outlined in this report. Therefore, achieving these outcomes will make a significant contribution to securing the social and economic contribution this industry plays across the UK.

# APPENDIX - OPERATIONAL RESILIENCE FRAMEWORK

To support the development of operational resilience as a discipline, PwC has created an updated framework which supports a business service-led approach.

The concept of operational resilience is evolving, and while some practices are established, overall frameworks require enhancement. To support this, we have developed our own view of resilience, founded on the basis of the past 'Dear CEO' and 'Spot Check' approaches and enhanced to factor in a new fundamental of operational resilience – the business service-led approach. Our framework is composed of three distinct parts:

- **Business services** – from the process of mapping through to the setting of impact tolerances.
- **Resilience capabilities** – the wide variety of capabilities required to underpin some or all business services.
- **Governance and standards** – the governance, management information, policies and standards that set out the firm's approach to resilience.

The articulation and fleshing out of business services is arguably the most significant new development for operational resilience. However, the effect on governance approaches and standards should not be underestimated. Senior management will require a wholly different perspective than previously, e.g. from the perspective of business services.

Many resilience capabilities may already be in place. However, these will still be required to be reviewed and updated to provide a seamless approach to resilience, updated for evolved regulatory requirements and to provide value to the firm as a whole.



## Governance & standards

1.

### Governance

The operational resilience strategy is aligned and embedded with the business and IT strategies. Operational resilience drives investment and risk decisions. The Board and Executive Management have accurate and adequate oversight of resilience activity, trends and remediation to assist them in making decisions.

2.

### Resilience framework and standards

An operational resilience framework is in place across the organisation, with clear definition and accountability for the different aspects of resilience. The framework is current, communicated and understood by the organisation.

## Business service view

3.

### Profiling

Mapping the business service end-to-end, across all functions.

4.

### Layering of enablers

Supplementing the overall business profile with details of the underlying technology architecture, property, personnel and third parties involved in delivering the service.

5.

### Key impacts identification

Identifying the metrics that can be used to understand the performance of a particular business services and whether issues are being experienced e.g. trade volumes, number of mortgage approvals, value of transactions.

6.

### Proving the profile

The process of running 'real' data through the business service profile and with the aid of past data, validating the use of the key impact metrics to understand business service performance.

7.

### Scenario development

The creation of 'severe but plausible' scenario narratives to enable effective stress tests. Scenarios should be articulated to a sufficient level of detail to make clear the issue and enable organisations to focus on the resulting effects.

8.

### Testing

The undertaking of periodic testing to deliver a view of the likely impacts of stress tests and also a sense of the consequential impacts of the stress scenarios across the organisation. Tests should be well documented and provide clear and actionable outcomes.

9.

### Impact tolerance calibration

The development and adjustment of impact tolerances for key business services, built on the creation, performance and analysis of stress tests. Tolerances should be set by business service and agreed by senior management.

10.

### Monitoring of performance

The on-going business as usual monitoring and reviewing of performance against impact tolerances, including the management of trigger alerts and escalation of potential issues.



## Resilience capabilities

11.

### Service operations

Technology services and processes have been designed so that they ensure continuity and there is appropriate investment in these processes and services.

12.

### Capacity management

Organisations can demonstrate through testing and monitoring the effectiveness of capacity measures.

13.

### Incident management

Incident response processes are in place to identify, classify and to help ensure appropriate, measured responses. Incident related MI helps drive strategic operational resilience decisions and investments.

14.

### Capability and resources

The organisation has sufficient skills and resources to deliver and help ensure operational resilience. There is a clear understanding of roles and responsibilities and the organisations operational resilience risks.

15.

### Sourcing and external dependencies

There is clear consideration and understanding of the dependencies on external or sourcing partners and the level of risk that is introduced into the critical services. Performance, risk and effectiveness of these relationships are frequently assessed and understood.

16.

### Risk management

An effective 3LOD model is in place whereby operational resilience risks are understood, assessed, monitored and communicated to the Board and Executive Management. Risk appetite for critical services have been defined and drive risk acceptance and risk mitigation activities. Risk MI assists in both strategic and tactical decisions.

17.

### Change management

Assurance and resilience is embedded in change control and SLDC activity where testing occurs across application development and infrastructure change. Well governed, documented change processes are in place and are fully understood by the organisation.

18.

### Continuity management

Appropriate continuity plans are in place for all critical services which are well understood by the organisation. These plans are reviewed and assessed regularly to help ensure successful implementation in a continuity scenario.

19.

### Physical security

To ensure that an organisation has the appropriate controls in place to manage physical access to business premises and that environmental quality factors are appropriately reviewed and within risk tolerance.

20.

### Cyber security

Cyber resilience mechanisms to prevent, detect, respond and recover from cyber-related threats are in place and aligned to the wider response and recovery capabilities.

[illegible]

## NOTES

[illegible]



## TheCityUK Research:

For further information about this report contact:

Simon Chard, Partner, PwC  
**[simon.c.chard@pwc.com](mailto:simon.c.chard@pwc.com)**  
**+44 (0)7740 241 051**

Hannah Swain, Director, PwC  
**[swain.hannah@pwc.com](mailto:swain.hannah@pwc.com)**  
**+ 44 (0)7803 590 553**

Marcus Scott, Chief Operating Officer, TheCityUK  
**[marcus.scott@thecityuk.com](mailto:marcus.scott@thecityuk.com)**  
**+44 (0)20 3696 0133**

Dominic Frost, Policy Officer, TheCityUK  
**[dominic.frost@thecityuk.com](mailto:dominic.frost@thecityuk.com)**  
**+44 (0)20 3696 0142**

---

# TheCityUK

TheCityUK, Salisbury House, Finsbury Circus, London EC2M 5QQ  
**[www.thecityuk.com](http://www.thecityuk.com)**

## MEMBERSHIP

To find out more about TheCityUK and the benefits of membership visit  
**[www.thecityuk.com](http://www.thecityuk.com)** or email us at **[membership@thecityuk.com](mailto:membership@thecityuk.com)**

This report is based upon material in TheCityUK's possession or supplied to us from reputable sources, which we believe to be reliable. While every effort has been made to ensure its accuracy, we cannot offer any guarantee that factual errors may not have occurred. Neither TheCityUK, PwC nor any officer or employee thereof accepts any liability or responsibility for any direct or indirect damage, consequential or other loss suffered by reason of inaccuracy or incorrectness. This publication is provided to you for information purposes and is not intended as an offer or solicitation for the purchase or sale of any financial instrument, or as the provision of financial advice.

Copyright protection exists in this publication and it may not be produced or published in any other format by any person, for any purpose without the prior permission of the original data owner/publisher and/or TheCityUK. © Copyright June 2019.