Deloitte.

# Resilience without borders

How financial services firms should approach the worldwide development of operational resilience regulation

CENTRE *for*
REGULATORY
STRATEGY
EMEA

# Contents

# Executive summary

- **Operational resilience** is an increasingly important and urgent priority for financial services regulators and is rising rapidly up the strategic agenda of financial services firms' boards and senior management teams. Firms are only beginning to understand the full extent of the demands that these emerging regulatory requirements will place on them, and their implications for their strategies and business models.

- **COVID-19 will accelerate the shift** in mindset that many regulators have adopted, towards asking firms to identify their most important business services, consider vulnerabilities to them that are broader than cyber-attacks and IT failures, and assume that severe disrputions will occur and lead to the failure of those services.

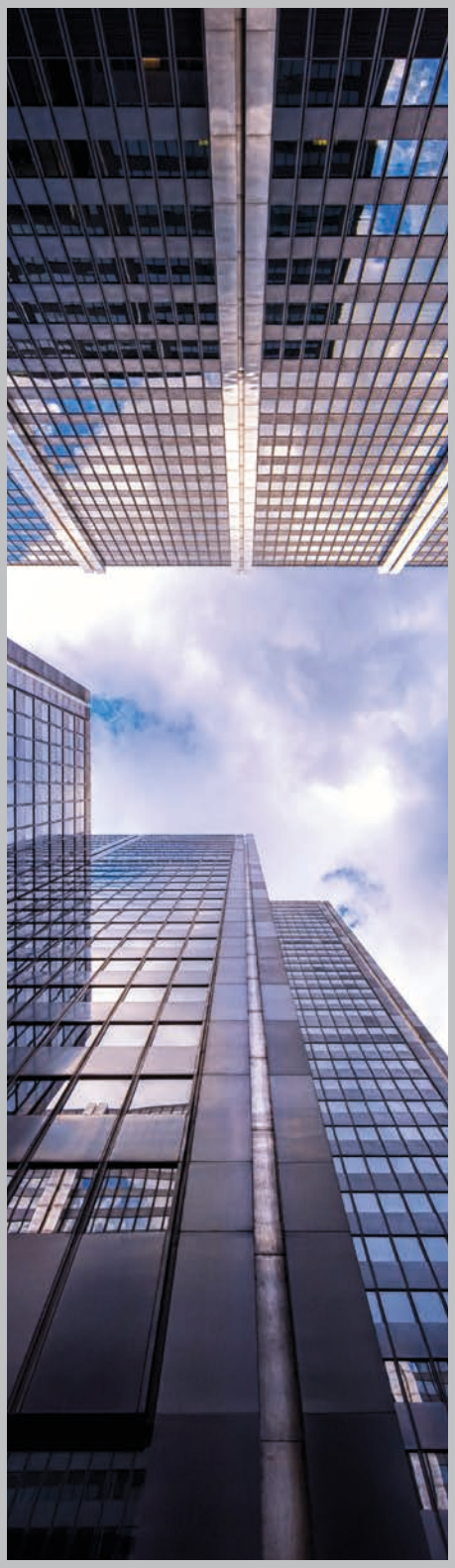
- **International standards and guidelines** for operational resilience in financial services are emerging, particularly with the Basel Committee on Banking Supervision's (BCBS) consultation on Principles for operational resilience. But international standards that exist or are being consulted on today are relatively high-level and give jurisdictional regulators considerable flexibility to develop their own distinct approaches.

- **Significant regulatory policy development** on operational resilience is now occurring at the national or jurisdictional level. New standards are being finalised, important and detailed consultations on supervisory approaches are in train, and in the EU, a significant legislative proposal on digital operational resilience is due soon. We have reviewed the most important and innovative regulatory policy developments that we see in the European Union, the United Kingdom and the United States.

- **Regulatory divergence** is a growing challenge for financial services firms, and divergence between national/jurisdictional authorities on the regulation of operational resilience is an important concern. Financial services groups will perform best, and be more resilient to unexpected operational threats, if they implement a consistent group-wide approach to managing operational resilience that is based on international leading practice.

- **We put forward our own outcomes-based framework** – our Key Attributes for enhancing operational resilience in financial services, drawing from the most ambitious and innovative regulatory and private sector approaches we have observed around the world. Our view is that a firm that bases its group-wide approach to operational resilience on these Key Attributes will be better placed to deal with evolving regulatory demands across jurisdictions going forward.

- **Recommendations on practical next steps** to enhance firm-level and system-wide operational resilience are included at the end of this report giving our view of where firms most urgently need to invest and what measures regulators and other public authorities could usefully take in the near term.



# **Introduction:** How financial services firms should approach the worldwide development of operational resilience regulation

The work of financial regulators has shifted significantly in recent years to include a much greater focus on the operational resilience of the financial system and of individual participants within it. Much of this has been driven by a growing awareness of the risks that could arise from the adoption of digital technologies and the interconnectedness of third parties. But operational resilience is, in fact, a much broader way of thinking about how the financial sector can plan for and respond to a wide range of non-financial events. Firms need to consider how these disruptions might harm their customers, jeopardise their own viability, or have knock-on consequences for other firms or the stability of the broader financial system.

Operational resilience is an area where both firms and regulators vie for leadership in the development of leading practice. Both are making significant efforts (and investments) to strengthen the financial sector's resilience. Recent events have demonstrated a **clear link between a firm's operational resilience and its ability to maintain the confidence of its customers, shareholders and the broader market** while being able to shift to new operating models. Being resilient to severe, and often unexpected, operational threats is an unambiguous good. Boards, management and regulators are becoming increasingly aligned in recognising its value.

### Finding the right approach to operational resilience

Operational resilience for the financial services sector does not at present benefit from one clear, detailed international standard that is meant to be adopted by regulators in all jurisdictions around the world. International standards covering some key concepts or practices do exist, and more are coming[1], but these are mostly principles and guidelines within which jurisdictional regulators have considerable flexibility to develop their own, distinct approaches. As a result, some of the most notable new regulatory initiatives on operational resilience have emerged in a 'bottom-up' way at the national level, rather than from the 'top down' post-crisis approach with which the sector is more familiar. This creates a real concern for internationally active firms that may, as a result, encounter mismatched requirements between jurisdictions that could make the adoption of a group-wide approach to operational resilience more difficult. The lack of an international framework is also an issue for primarily domestic firms as it makes it less predictable how certain requirements might develop locally.

**Defining operational resilience:**

*"Operational resilience is the ability of a [financial services firm] to deliver critical operations through disruption. This ability enables it to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption."*

BCBS consultative Principles for operational resilience, August 2020

This is not an insurmountable problem for financial services firms. Our view is that firms can find a path through these different national approaches and requirements, and that by doing so can strengthen their operational resilience considerably, by adopting a group-wide approach anchored in an outcomes-based resilience framework. This framework should draw on widely recognised standards such as ISO 22301 Business Continuity Management Systems and leading jurisdictional practices from around the world, especially when they are or appear to be in line with the direction of travel pointed to by international standard setters, such as the BCBS August 2020 consultative Principles on operational resilience.

To help firms do this, this report includes our own outcomes-based framework; **the Key Attributes for enhancing operational resilience in financial services.** We have based this framework on the following five attributes:

1. **Understanding the risk perimeter**
2. **Understanding the impact of disruptions**
3. **Setting tolerances for disruptions**
4. **Effective incident coordination**
5. **Effective ex-ante testing**

### The value of a globally consistent approach for firms

The services offered by financial services firms will often be supported by other firms (both affiliates and third parties), people, systems and processes that are in multiple jurisdictions. Firms need to think carefully about how to handle the different requirements that their regulated entities are subject to, as well as reconciling their compliance duties with their existing global management systems for operational risk, business continuity, and recovery and resolution planning.

Financial services firms can often face a large operational burden from overlapping or duplicative requirements put forward by different regulators. EU regulators, for instance, have recognised[ii] that existing incident reporting requirements are insufficiently streamlined, using different terminology and timeframes, and requiring different levels of detail. Potentially more challenging, however, is when regulatory requirements are substantially different due to a jurisdiction's preferred approach, area of focus or scope. Firms are already seeing this with the UK's focus on the delivery of important business services while some other jurisdictions continue to focus primarily on the strengthening of controls around key technology assets.

In these cases, there is a real risk that internationally active firms will struggle to achieve resilience-by-design and substitutability in their service provision. Given the cross-border interdependence of service delivery, the resilience of a firm's services in one jurisdiction will often depend on the supporting assets or processes located in other jurisdictions being equally as strong. **Taking a group-wide approach to planning for operational resilience will give firms more opportunities to 'plug the gaps' between jurisdictional approaches beforehand;** and to reconcile inconsistencies in a way that becomes more operationally efficient and cost effective, as well as strengthening their own resilience to operational threats.

To deal with this, cross-border firms should adopt international leading practice group-wide, even if local regulators only require some of their units to do so. This report reviews the most recent regulatory developments on operational resilience in the EU, the UK and the US. We then draw on the most successful and innovative approaches we observe to develop our Key Attributes framework which we believe firms can use as a guide to design and implement their group-wide approach.

Taking the initiative in this way can often be a beneficial strategy and the private sector is already leading the way in some areas of operational resilience. In the US, the leading role that firms, often working through industry bodies, have taken on cyber resilience in the last ten years has led to some of the most sophisticated simulation exercises and burden sharing mechanisms in the world. Our view is that the financial industry should aim to take a similarly leading role in more areas of operational resilience.

### Why firms should do more than the minimum on operational resilience

We have written previously about the commercial rationale for firms investing in their operational resilience. In our 2019 paper **'On the Frontier: Operational resilience and the evolution of the European banking sector**' we noted that, in our experience, a firm's operational resilience is often a decisive feature of its ability to remain competitive in an increasingly digitally enabled market.

Taking the initiative in this way can often be a beneficial strategy and the private sector is already leading the way in some areas of operational resilience.

The worldwide regulatory direction of travel is also important to consider. Although individual countries are moving at different speeds, we are seeing a widespread shift in regulatory policy across the major jurisdictions to prioritise the operational resilience of the financial sector and its most important firms. Current events are expected to accelerate this momentum. Firms that adopt international leading practice group-wide are likely to put themselves in a better position going forward to show regulators, shareholders, external and internal stakeholders that they have done the hard work to build their resilience, even if it means that some of their units will be 'super-compliant' or 'pre-compliant' with local rules (where they exist and are relevant) for a period of time. This report includes an 'In focus' section [on pg. 15] looking at service failure scenario testing to demonstrate how a global approach can be helpful in reconciling different regulatory requirements. This could also drive differentiation in the market with clients and consumers.

**The experience of the financial sector with COVID-19 and the world's pandemic response has shown us that those firms which were more advanced in adopting leading practices similar to the regulatory approaches on operational resilience being developed today performed better in lockdowns.**

Moreover, these firms are presently better prepared to handle the challenges that may arise in the next stages of the response. This is particularly the case with those firms that had a stronger understanding of their important business services, the resources that supported their delivery, and had a clearer idea of the kinds of harm to customers, clients and counterparties that could arise if those services were interrupted.

To complement the rationale of the Key Attributes with more practical steps, this report concludes with a number of recommendations, directed to both firms and regulators, on important areas for action in order to strengthen the operational resilience of financial services in future. These recommendations should help firms think about the areas where investment in their operational resilience is most urgently needed, and how making these investments can also lead to achievable commercial benefits, such as enabling their digital transition and competitiveness.

## **In focus:** The impact of COVID-19 on the financial services policy approach to operational resilience

The COVID-19 pandemic and the resulting changes to economic and social activity are testing the financial sector in many ways and accelerating discussions on operational resilience. One of the most prominent tests, especially in the earlier stages of the pandemic response, was of its operational resilience. A sudden and widespread shift to remote working meant almost every firm had to alter the way it delivered services to its customers, often through digital channels or at a distance rather than in-branch or in-person.

From an operational point of view, for the most part, the financial sector handled the first stage of the pandemic remarkably well, with limited disruption to core services. For this, both firms and their regulators deserve a great deal of credit. But this should not lead to a sense of 'job done' when it comes to the operational resilience of individual firms or the financial sector as a whole.

While COVID-19's effects have been historic in their sheer scale, they do not represent the most challenging operational disruption the financial sector could plausibly face. Comparing COVID-19 to some of the operational disruptions regulators had been considering before the pandemic (most notably, disruptions to firms' access to market infrastructures or widespread data corruption/availability events) the latter could threaten firms' ability to deliver core services to their customers for a more prolonged period of time than a shift to home working.

**Lessons we believe will emerge from the COVID-19 experience**
The experience of COVID-19 will undoubtedly influence the direction of regulatory policy on operational resilience in financial services. Regulators in the EU, UK and US will all have opportunities in the coming months to reflect lessons learned in how they design their approach to this issue (most notably in the EU, where the European Commission has decided to prioritise the proposal of the Digital Operational Resilience Framework (DORF) as part of its COVID-19 recovery strategy).

In our view, there are at least three important lessons from COVID-19 that stand out as critical for regulators and firms to reflect in their thinking going forward:

- **The scope of risks considered:** COVID-19 has shown that scenarios not directly related to technology failures can bring about serious challenges to operational resilience. Even though IT risks will likely remain the most frequent threat to operational resilience in financial services, this experience demonstrates that firms should be conducting resilience planning based on a wide range of public health, public infrastructure, environmental and other scenarios that affect the operating model through which business is conducted. Authorities in jurisdictions that have focused mainly on cyber threats to the financial sector as the most likely source of an operational systemic disruption may choose to broaden their scope of analysis.

- **A services view of resilience:** the pandemic demonstrated that a focus on identifying, understanding and maintaining important business services, in addition to protecting key assets, can be a more effective approach to dealing with an unexpected and unconventional resilience shock than asset protection. Worldwide lockdowns did not directly threaten the integrity or connectivity of a particular IT or infrastructure system, but instead challenged firms to continue their core operations, through modified procedures and the use of substitute channels, just when daily life had to change dramatically. Focusing on the adaptability and alternative delivery of important business services is a critical part of operational resilience thinking. We are also seeing regulators respond to the experience of COVID-19 by increasing their focus on the resilience of third party suppliers as well as the role of significant infrastructure and technology providers.

- **System-wide threats are very plausible:** the COVID-19 experience is showing that some of the most important threats that the sector needs to plan for are not always idiosyncratic. Large, system-wide and interconnected events that threaten the functioning of financial markets, or the economy as a whole, happen with sufficient frequency that they need to be taken seriously, even when crises become a distant memory. This is not solely the responsibility of governments, security agencies and regulators. Emerging regulatory frameworks are increasingly putting the onus on firms to plan their response to these 'wide area' events and consider how disruptions to their core services could endanger the systemic stability of the financial sector. In the current circumstances, a significant second wave of COVID-19 infections in some regions is a potentially severe and very plausible scenario that firms need to be preparing themselves for now.

# **Review:** Jurisdictional approaches to financial services operational resilience

This section reviews the frameworks in the EU, the UK and the US for the operational resilience of financial services, both at the level of individual regulated firms and system-wide. We focus both on existing frameworks and on current developments that we believe are the most indicative of the regulatory direction of travel in each jurisdiction.

The analysis in this section should serve as a guide for firms looking to understand where there are most likely to be gaps and inconsistencies in the approach, scope or maturity level of these regulatory frameworks. This analysis supports the Key Attributes framework that follows describing leading practices for the management of operational resilience risks.

### How we approach the review of each jurisdiction's framework

The review in this section employs a broad scope in order to ensure we capture different approaches in each primary jurisdiction. Where certain regulators have developed an approach looking only at cyber risk in financial services, rather than operational resilience more broadly, we have still included it for its value to that narrower set of risks.

Finally, to ensure the relevance of our analysis to the policy development currently being undertaken by regulators in all jurisdictions, we have considered non-final regulatory approaches that have been articulated with a high level of detail, but which may not be fully settled or implemented. This means that we have taken into account the UK's operational resilience framework, on which UK authorities have consulted at a high level of detail, but not the EU's forthcoming DORF, for which there is presently no certainty in terms of the EU's eventual expectations for firms (although we expect the legislative proposal to be published shortly).

### European Union

The EU's regulatory approach to operational resilience in financial services has so far been a patchwork of different initiatives and priorities driven by numerous regulators and public authorities. In addition, several EU Member States have led in the development of some attributes of operational resilience regulation (such as the Netherlands on red-team penetration testing). An upcoming legislative proposal from the European Commission (the DORF) has the ambition to standardise the approach taken by financial services regulators and to adopt leading national practices bloc-wide.

The EU currently follows a sectoral approach, with different rules, standards or guidelines – that are sometimes, but not always, similar – in place for banks, financial market infrastructures (FMIs), insurers, and other capital markets participants. For instance, the European Central Bank (ECB) has developed Cyber Resilience Oversight Expectations (CROE)[iii] for FMIs, which are materially different to the European Banking Authority's (EBA) Guidelines on ICT and Security Risk Management[iv], applicable to banks, investment firms and payment service providers. The EBA's Guidelines are similar but different and separate from the European Insurance and Occupational Pensions Authority's (EIOPA) Guidelines on Information and Communication Technology Security and Governance[v].

This fragmented approach between authorities has not stopped the emergence of some advanced standards. TIBER-EU, a non-binding red-team penetration testing framework developed by the ECB[vi], has seen a slow but steady uptake by regulators in several Member States. The EBA and EIOPA Guidelines, and the CROE for FMIs suggest TIBER testing be used as a supervisory tool. However, such testing is not always mandatory, and its implementation by national authorities still needs to become more consistent and frequent. If a more consistent approach cannot be achieved, there is a risk that current cyber maturity disparities between EU Member States will be exacerbated, with knock-on consequences for the overall cyber security of the European financial sector. It is notable, however, that the EU's work on testing to date does not extend to testing against other operational resilience threats outside cyber risks.

The often nationally led approach can also be seen in the EU's lack of multi-sector, bloc-wide market coordination groups and information-sharing protocols, something that may affect firms' ability to share threat information, and authorities' capacity to coordinate effectively when incidents occur. This may change with the European Network Information Security Agency (ENISA), the EU's cybersecurity agency, expanding its role as a facilitator of leading practice or through an initiative included in the DORF. However, as it stands, FMIs are the only EU sector that has started systematically sharing cyber threat-information, with the recent launch of the Cyber Information and Intelligence Sharing Initiative (CIISI-EU) by the ECB's Euro Cyber Resilience Board[vii].

The EU's work in financial sector operational resilience has, for the most part, been focused on cyber or IT risk rather than broader resilience threats. The upcoming legislative proposal for the DORF, with its focus on 'digital operational resilience' will broaden this scope. The DORF may also usefully opt to extend standards and programmes currently only in place for FMIs to the financial sector more broadly. It could also streamline existing rules, including on incident reporting and requirements on ICT and security risk management. Importantly, EU officials have also indicated that the DORF will look at developing an oversight framework for third-party providers (TPPs), especially cloud-service providers (CSPs) that are considered critical to the delivery of financial sector services. The format of this oversight regime is still open (we understand that the approaches currently being discussed include direct oversight and a certification regime). It is important to note, however, that after the DORF legislation is proposed by the Commission, it could spend a year or more in political negotiations, and any certainty on its eventual contents is still some way off.

The European Systemic Risk Board (ESRB), the EU's macroprudential oversight agency, has recently signalled[viii] an increasing focus on the potential systemic risks to the financial sector that could arise from cyber threats. It has suggested mitigants, including cyber stress testing programmes and a data vaulting scheme (two other tools currently absent from the EU's financial services regulatory arsenal). It remains to be seen how – or whether – these will be adopted through the DORF or other initiatives.

### United Kingdom

The UK is set to be the most unitary and centralised system of the three jurisdictions we analyse in this report. Its maturing operational resilience framework is based on a nearly-developed approach that is still under consultation[ix], but that will likely be implemented over the next three to four years.

This centralised institutional approach has meant the UK has been able to designate a body, the Financial Policy Committee (FPC), that is chiefly responsible for assessing the macro-operational risks to the financial system, and coordinating the work of regulatory agencies to respond to the risks it identifies. This facilitates authorities' understanding of the risk perimeter and in measuring industry-wide impacts. UK regulators also facilitate several cross-market cooperation platforms for financial services operational and cyber resilience: the Cross Markets Operational Resilience Group (CMORG), the Cross Markets Business Continuity Group (CMBCG)[x], and the Financial Sector Cyber Collaboration Centre (FSCCC)[xi], that are all crucial in sectoral incident coordination. Its cyber penetration testing regime is also among the most advanced in the world, with 'core' firms required to carry out these ex-ante red-team tests at regular intervals. UK regulators have also begun to develop an approach to stress testing firms based on operational disruption scenarios, the pilot of which was carried out in the summer of 2019.

The operational resilience framework presently being developed by UK regulators differs to the approach taken by EU and US authorities insofar that its focus is not critical asset protection, but the delivery of important business services. It requires firms to understand their most important business services, what systems and processes underpin them and what stakeholders they serve, and focus on the resilience of those services to severe but plausible scenarios. Importantly, the framework puts the board front and centre, asking it to sign off the impact tolerance statements for these business services. This is in addition to the existing accountability regime, the SM&CR[xii], where the SMF24 Chief Operations function will be responsible for implementing the framework. The emphasis placed by UK regulators on the governance of a firm's operational resilience is expected to increase the resilience of individual firms through encouraging better investment decisions. It should also help authorities understand better the system-wide risks and interconnections, by having an aggregate view of the individual submissions firms make.

As the UK operational resilience framework is finalised and implemented, authorities will have to reflect whether the regulatory perimeter needs to be expanded, perhaps to include some TPPs – a step the UK parliament has suggested the FPC consider recommending if TPPs are deemed to be systemic, and if concentration risk among them is considered too high. UK authorities will also have to do further work to develop their nascent operational disruption stress testing regime. The pilot exercise in 2019 was based on payment systems becoming unavailable to participating firms (which was, despite its 'cyber' label, in substance an operational resilience test). Further testing may focus on data integrity threats, although the timing and details of the next steps are not yet clear. These tests, if further developed, have the potential to become a significant part of the regulatory approach to operational resilience, akin to the role that financial stress testing plays in understanding a firm's capital adequacy.

UK authorities are also considering how they might act to facilitate the development of a safe harbouring scheme. Regulators are already discussing this with market participants, and market-driven solutions to sector data storage and recovery could develop in the medium term.

## United States

The US' regulatory framework for operational resilience is still developing across banking and securities regulators given the regulatory structure. It currently functions largely through a market-led approach informed by high-level principles, requirements and expectations set by various financial services authorities in statements and guidance. The US has advanced levels of cross-market and agency cooperation, but less developed rules and principles to rely on for supervision and enforcement, for instance on the setting and evaluation of operational risk tolerance for firms that includes a view on operational resilience. This is in part because it is still defining through what lens – and using which means – to implement rules on firms' approaches to operational resilience.

The US's approach has its underpinning on the banking side with the long standing Federal Financial Institutions Examination Council's (FFIEC) information handbooks that include coordination among the federal banking agencies. These standards and guidance that exist largely focus on discrete elements such as third party vendor risk management, business continuity, information security and cybersecurity. The most important are the FFIEC IT handbooks[xiii], individual regulatory agency guidance, the Financial Services Sector Coordinating Council (FSSCC) Business Services Resilience and Restoration white paper[xiv], and the Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations Cybersecurity and Resiliency Observations paper[xv]. However, this has led to a multiplicity of often overlapping requirements and guidelines that firms need to consider across banking and securities regulators. This is widely considered by industry[xvi] to take up a majority of the resources that many firms can dedicate to resilience functions and is often said to have encouraged a tick-box approach to complying with these rules, for example when evaluating the risk perimeter or setting tolerances for disruptions.

The US Federal Reserve Board (FRB) has an overarching role in setting regulatory policy for large financial institutions, community and regional financial institutions, FMIs, foreign banking organisations (non-US headquartered) and consumer compliance while the Financial Stability Oversight Council (FSOC) can act as a macro-operational oversight body. It remains to be seen, however, to what extent the FRB and FSOC will be able and willing to intervene to create a more streamlined approach to operational resilience regulation among authorities.

Senior US regulators have nevertheless recognised that 'the fragmented regulatory landscape for cyber risk and lack of mature metrics and measurement tools add difficulty'[xvii] to the management of cyber and IT risks in the financial sector.

The US's appetite for a wholesale shift from a more cybersecurity focused approach to an operational resilience perspective has yet to crystallise. The 2020 Office of the Comptroller of the Currency (OCC) and Federal Deposit Insurance Corporation (FDIC) Joint Statement on Heightened Cybersecurity Risk[xviii] did outline the issue is not one for the cybersecurity function to manage in a silo, and that business continuity plans (BCPs) could incorporate 'elements necessary for recovering from a cyber event'. However, its focus remains on cybersecurity. We increasingly see US supervisors individually push firms to consider wider threats to their business services and to break down internal silos across business continuity planning, information technology, operational risk and third party risk management. Despite this, on paper, the regulatory approach has not fully laid out its expectations for how firms should be planning for disruptions to their business services more widely, how firms should recover from these disruptions, and demonstrate their ability to operate going forward. The recent BCBS Principles for operational resilience, however, indicate that this might be changing given US membership of and the role it traditionally plays in that group.

The most notable strength of the US operational resilience framework is seen in its partially privately-led approach to cooperation, coordination, and testing in the financial services industry. It is the only one of the three jurisdiction we examine that has a burden-sharing solution based on an established shared data vaulting scheme (Sheltered Harbor[xix]) which can activate data backups, potentially using another firm's infrastructure, to provide customers with access to services and accounts following a catastrophic cyber attack. It also runs extensive market coordination and crisis simulation exercises through the Financial Services Information Sharing and Analysis Center (FS-ISAC)[xx], the Securities Industry and Financial Markets Association's (SIFMA) Quantum Dawn exercises and others[xxi]. Together, these exercises enable firms and authorities to test their coordination in the case of a severe incident, check individual response capabilities and understand the potential system-wide implications of cyber and operational incidents.

"While significantly higher levels of capital and liquidity have improved banks' ability to absorb financial shocks, the Committee believes that further work is necessary to strengthen banks' ability to absorb operational risk-related events, such as pandemics, cyber incidents, technology failures or natural disasters, which could cause significant operational failures or wide-scale disruptions in financial markets."

BCBS consultative Principles for operational resilience, August 2020

## BCBS Principles on operational resilience

On 6 August 2020, the BCBS issued a consultation on 'Principles for operational resilience' to give more guidance to banking regulators developing their approach in this field. While the BCBS Principles are relatively high-level and do not provide a detailed template for a regulatory and supervisory framework, they do set out what the BCBS considers to be a minimum set of areas that banking regulators should address in their future work. The areas where the BCBS is proposing to develop its Principles are:

- **Governance:** placing the onus on the board to review and approve the bank's operational resilience planning and risk tolerance.
- **Operational risk management:** stressing the need for cross-functional cooperation to identify and manage vulnerabilities to critical operations.
- **Business continuity planning and testing:** requiring banks to put in place business continuity plans for critical operations and validate them with business continuity exercises using severe but plausible disruption scenarios.
- **Mapping interconnections and interdependencies:** to a level of granularity sufficient for banks to assess their ability to stay within their risk tolerance during a disruption.
- **Third party dependency management:** highlighting the importance of TPPs as well as intra-group entities in creating dependencies that could threaten critical functions if disrupted.
- **Incident management:** requiring banks to have incident recovery plans for critical operations, covering incident identification, incident management procedures and communications planning.
- **Information and communication technology including cyber-security:** emphasising the importance of linking the identification of critical information assets and their cyber protection with the impact their failure could have on a bank's critical operations.

The consultative Principles outlined by the BCBS are an important indicator of the regulatory direction of travel that banks (as well as other financial services firms) can reasonably expect to see in the jurisdictions where they operate, especially where those jurisdictions are BCBS members. In our view, these Principles are most closely aligned to the approach UK regulators are taking to operational resilience and provide further evidence that new practices and concepts such as critical service identification, risk/impact tolerance setting, and service failure scenario testing are gaining in acceptance elsewhere as leading practices.

# **Framework:** Our view of the Key Attributes of operational resilience in financial services

We have developed the Key Attributes framework in this section based on our understanding of the most important elements of operational resilience, and drawing from the most ambitious and innovative regulatory and private sector approaches we have observed around the world (those both in place and under development). This analysis has also been informed by regulatory practices that are based on widely accepted international standards, such as ISO 22301 Business Continuity Management Systems, and where those practices have been, or are in the process of being, taken on by global bodies, such as the BCBS's recent consultative Principles on operational resilience.

As a result, our view is that a firm that bases its group-wide approach to operational resilience on our Key Attributes framework would bring its activities in line with the BCBS Principles on operational resilience and go some way towards preparing the firm to meet local regulatory requirements in many jurisdictions. By contrast, a firm that based its approach to operational resilience directly on the BCBS Principles would still be likely to face more challenges complying with regulatory requirements in the UK, EU and US. This is because the BCBS draft Principles alone would not fully prepare the firm for certain emerging practices (such as service failure scenario testing or expressing risk tolerances from a customer harm, firm viability or financial stability perspective in the UK).

### Operational resilience at the firm and system-level

An important characteristic of operational resilience is that there are factors supporting resilience at an individual firm level and factors that can only be developed among a group of firms or market-wide. This is similar to financial resilience where regulators focus on both micro-prudential and macro-prudential objectives. As a result, we have built our Key Attributes framework on five attributes, with each attribute being described on two levels:

- **An operational resilience framework for firms:** this comprises the individual actions firms should take to build and maintain their resilience, preferably, where possible, at a group-wide level.

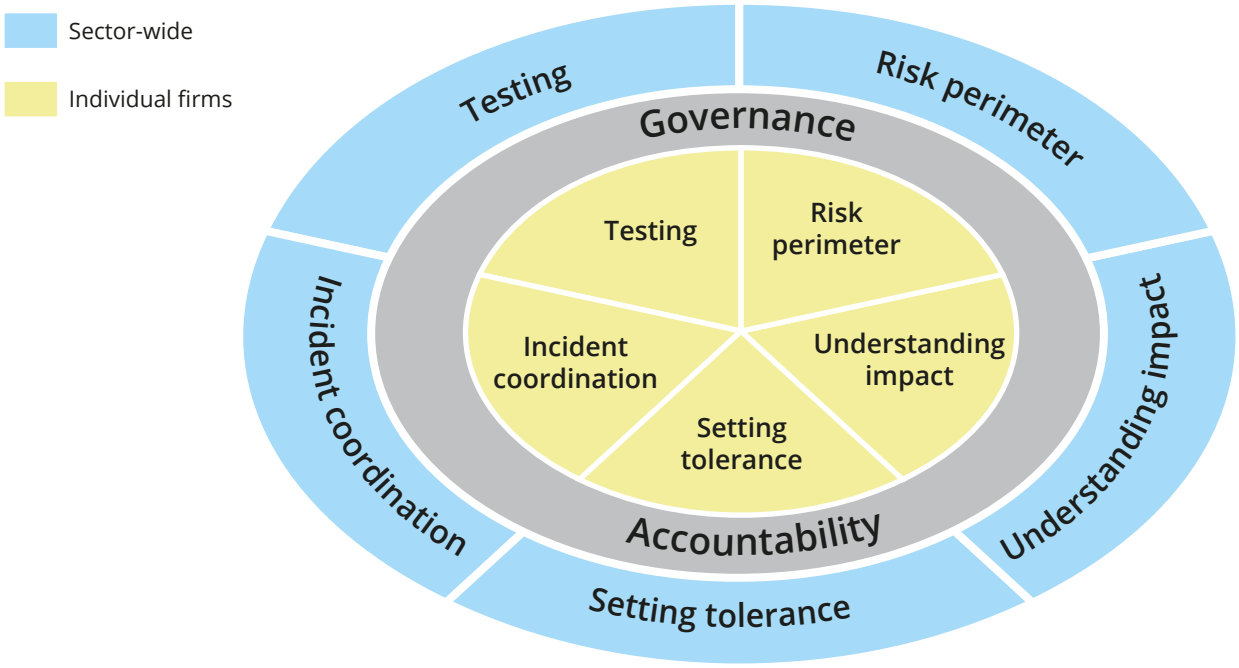
- **Sector-wide resilience characteristics:** these are the market-wide initiatives, groups, protocols and regulatory interventions that strengthen the resilience of the sector as a whole to operational stressors. They can be developed either by the industry acting on its own initiative, or with some level of partial or full regulatory direction.

### The governance of operational resilience

Across all of the five Key Attributes we see the governance of operational resilience in firms and establishing clear accountability for operational resilience outcomes as a rapidly emerging part of almost every regulatory approach observed, and one that supports all of the five Key Attributes in some form. Here, the regulatory direction of travel is to emphasise the clear ownership of operational resilience by senior management, or more likely, by the board. This approach, recently reflected in the BCBS Principles, places a strong emphasis on the board's responsibility for reviewing and signing-off on its firm's operational risk tolerance, ensuring that appropriate funding and resources are made available in order to support the investment in resilience needed to meet that tolerance, and regularly receiving reports from senior management on operational deficiencies or about events where risk tolerances were, or came close to being, breached.

An important characteristic of operational resilience is that there are factors supporting resilience at an individual firm level and factors that can only be developed among a group of firms or market-wide.

**Figure A: The Key Attributes for enhancing operational resilience in financial services**




## A more detailed look at our Key Attributes for enhancing operational resilience in financial services

| | Operational resilience framework for firms | Sector-wide resilience characteristics |
|---|---|---|
| Understanding the **risk perimeter** | Firms identify their most important business services, including what external connections exist that feed into them, and where the business services feed out into the ecosystem. Further, firms seek to understand the process dependencies that underpin these services, both internally and externally with TPPs, the defensive controls in place to protect them, and the areas where further investment is most needed. | Authorities have a 'macro-operational' body in place that is able to assess how individual risks compound into system-wide risks. There are powers in place that enable oversight of TPPs when necessary. An agency coordination group is set up to discuss the implications of evolving threats, vulnerabilities, and their potential consequences. Finally, a central body is established either by authorities or by sectoral associations to assemble and provide information on active threats. |
| **Understanding the impact** of outages and disruptions | Firms seek to understand the vulnerabilities to their business services to which internal and external dependencies give rise. They understand how disruptions to their business services may affect their relevant stakeholders, ranging from harm done to retail customers to threatening the functioning and stability of financial markets. | Authorities are able to assemble a comprehensive picture of the macro-operational risks and likely harm to the sector and its stakeholders arising from the disruptions to individual firms' business services that appear most likely, based on known and anticipated threats and vulnerabilities. The authorities communicate their assessment of the resulting risks. |

| | Operational resilience framework for firms | Sector-wide resilience characteristics |
|---|---|---|
| **Setting tolerances** for outages and disruptions | Firms set risk tolerances for disruptions to their business services, and establish service contingencies to maintain their business services based on these risk tolerances. They should have plans to continue services through disruption including through effective internal backups. Firms should consider, where possible, setting expectations by publishing these risk tolerances, indicating the service levels stakeholders can expect in the event of a disruption. | Authorities make use of the macro-risk analysis to set policy accordingly. Their starting point is that operational failures will occur and cannot be avoided with any amount of planning. They promote the development of cross-sector recovery protocols that can be actioned, including in the most extreme disruptions to the operations of the financial services sector (i.e. existential events beyond the 'severe but plausible' level to which they expect firms to be resilient). |
| Effective **incident** coordination processes and tools | Firms have detection and escalation processes in place for when disruptions or near misses occur, and are then able to trigger their service contingencies and potential cross-market defence/ mitigation mechanisms. Firms have effective internal and external communication plans that can help stakeholders access alternative service delivery methods. Firms report resilience threats in good time to regulators and engage in a sufficient level of cross-sector information sharing. | The sector-proactively coordinates its understanding of and response to resilience threats as they arise. Cross-sector backup mechanisms are established to share the operational burden of crises in order to limit the likelihood of threats becoming systemic. |
| Effective ex-ante **testing** | Firms carry out simulated threat exercises such as penetration testing on live production systems (e.g. CBEST, TIBER) and regular crisis simulation exercises. Firms develop scenario-based service failure exercises to understand better the level of resilience they have attained for their important business services. Firms take action on lessons learned from these tests. | Authorities participate in international coordination and crisis exercises, and organise public-private exercises in their local jurisdictions that bring together a broad representation of important financial services firms and critical infrastructure providers. Authorities also develop operational resilience stress testing programmes for the most important financial services firms they regulate. Authorities take action on lessons learned from these exercises. |

## **In focus**: Singapore's approach to financial services operational resilience

With Asia-Pacific markets becoming even more prominent in FS firms' geographic reach, the regulatory approaches taken there are of increasing importance as they consider their group-wide regulatory strategy. Global regulatory divergence is a growing trend that we have written about extensively in the last few years, but for the most part APAC regulators, certainly those which are members of the Financial Stability Board (FSB), have been assiduous in their national implementation of global standards. In the field of operational resilience, APAC authorities seem similarly open to adopting international leading practice in the design of their regulatory frameworks.

In 2019, the Monetary Authority of Singapore (MAS) set out its approach to operational resilience by publishing a consultation paper on revised Guidelines on Business Continuity Management. The approach proposed by the MAS reflects many of the elements contained in our Key Attributes. This consultation also represents a significant step change in how the MAS has hitherto thought about operational resilience. The MAS extended its thinking to go beyond BCPs for specific and isolated events to focus, more broadly, on how firms plan for and respond to a wider range of scenarios that could adversely affect their customers, undermine their own viability and the sector's stability.

Our assessment is that the framework contained in the 2019 Guidelines reflects:

- **Use of leading practice:** having monitored international developments in the field of operational resilience, MAS has decided to adopt what it sees as leading international practice. Other jurisdictions in the region may opt for a similar approach.
- **An opportunity for compatibility:** firms that adopt a group-wide approach to operational resilience based on our Key Attributes may find jurisdictional rules more compatible with each other, as shown below:

**UK approach**

- The proposed UK operational resilience framework requires firms to identify important business services.
- Firms would also need to identify, and document resources required to deliver each of their important business services. This process is referred to as 'mapping'.

**Key Attributes – Understanding the risk perimeter**

- Firms identify their business services, including what external connections exist that feed into them, and where the business services feed out into the ecosystem.
- Firms seek to understand the process dependencies that underpin these services, both internally and externally with TPPs, the defensive controls in place to protect them, and the areas where further investment is most needed.

**Singapore's approach**

- The consultation re-defines business functions based on the services provided to customers.
- Firms will have to develop an end-to-end business continuity plan for each critical business service.

The similarities to the Key Attributes extend beyond understanding the risk perimeter, and remain true to our core operational resilience concepts even when superficially different. Indeed, although the MAS Guidelines do not contain explicit guidance on how the annual tests of BCPs should be conducted, they do require firms to develop BCPs that 'can address a broad range of plausible scenarios from wide-area disruptions to pandemics'. Another example is the MAS requirement that BCPs for important business functions be audited annually. This is superficially different to the UK's requirement to conduct self-assessments, but requires the same underlying work and aims to achieve the same objectives – asking firms to check whether their operational resilience arrangements are fit for purpose.

These similarities, along with other comparable requirements that encourage participation in public-private exercises, or setting 'minimum performance levels' – akin to the UK's impact tolerances – show increasing convergence, in substance if not in form, between the regulatory approaches to operational resilience taken by supervisors in two major financial centres. This further underscores the opportunity internationally active firms have in adopting a group-wide outcomes-based approach to assessing and strengthening their operational resilience.

## **In focus**: Cross-border service failure scenario testing in an insurance firm

Developing a credible approach to scenario testing is an important part of managing operational resilience. This demonstrates to boards, senior management and to regulators that a firm is able to recover its important business services to an acceptable level after suffering a severe but plausible disruption to normal operations.

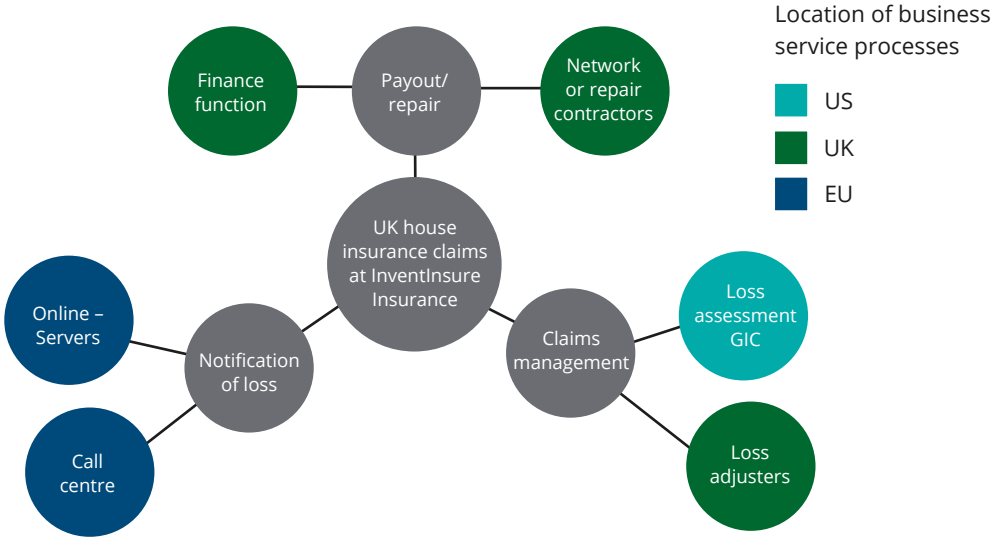
While service failure scenario testing (SFST) appears likely to soon become a regulatory requirement for financial services firms in the UK, our Key Attributes framework argues that firms can benefit from adopting these programmes at a group-level.

The hypothetical example below shows how an internationally active insurer based in the UK delivers an important business service to its customers that is underpinned by a cross-border value chain of processes located in the US and Eastern Europe, each with its own operational vulnerabilities. While the UK regulatory approach requires intra-group services to be included in SFST, we believe there is an opportunity here for financial services groups to take a much more robust approach with a wider scope of entities and one that uses disruption scenarios involving multiple events occurring across geographies. In our view, the insurer in this example would not only conduct a more meaningful exercise for the resilience of the group as a whole, but it could also make an important contribution towards complying with EU and US regulatory requirements that have a different primary focus. Taking a narrower approach by only including third country functions that directly support UK services would be less useful for the group's operational resilience activities outside of the UK. By contrast, taking a global approach to SFST could help the EU entities in the group identify their critical business processes and activities, business functions, and roles and assets (as required by EIOPA's draft Guidelines on ICT security and governance). The group's entities in the US could equally leverage the exercise to complete the business impact and business continuity work required by their State regulators.

**Figure B: Important business service failure scenario testing**

**Impact tolerance:** be able to settle simple claims within 48 hours.

**Scenario:** major hurricane in US floods the loss assessment Global In-house Centre (GIC) and a state-sponsored cyber attack in Eastern Europe affects call centre ability to receive calls.




Facing this severe but plausible scenario, the operational resilience of this insurer's claims function relies on dependencies spanning three continents. Taking a narrow view in evaluating the operational resilience of the UK service alone (that is, evaluating foreign intra-group functions and using simpler local disruption scenarios) would create little scope for group-wide learning. This would also, arguably, come at a larger overall cost over time if further testing requirements develop in other jurisdictions. Taking a group-wide approach to the SFST exercise early on, specifically one that is designed to accommodate local regulatory requirements within a larger framework, would enable the insurer in this case to:

- build a higher level of group-wide operational resilience, at a diminishing marginal cost for jurisdictions included;
- help comply with varying regulatory obligations, either directly or indirectly, using a single approach; and
- facilitate the design and transformation of operating model strategies by highlighting possible cost-saving opportunities, and having a more holistic understanding of the operational functioning of the entire group.

# **Recommendations:** Key actions for firms and regulators

Firms and authorities are now at a critical point in the development of their approaches to the operational resilience of the financial sector. Significant proposals on the overarching regulatory framework for operational resilience are in-flight in several jurisdictions, and the outcome of those proposals will guide regulatory action in financial services for the foreseeable future.

Moreover, following the experience of COVID-19 and the resulting restrictions on activity, operational resilience is rising up the strategic agenda of financial services firms' boards and senior management teams. Decisions taken today on investments to be made in resilience capabilities will determine how effectively a firm will be able to navigate future regulatory expectations and scrutiny in this area.

In our view, both the public and private sector need to take a number of actions in order to succeed in strengthening the operational resilience of the financial sector. In this section, we include two sets of recommendations for each of our five Key Attributes of operational resilience:

**Actions for firms:** based on our view of the likely development of regulatory demands, actions that firms should take, both individually and collectively in industry groups, to strengthen their resilience and address regulatory framework gaps, where they exist.

**Actions for public authorities:** based on global leading practice, what public authorities can do to strengthen their operational resilience framework domestically and promote regulatory convergence and consistency between key jurisdictions.

## Risk perimeter

### Actions for firms:

- **Business service identification:** firms should attach a high priority to identifying the important business services they offer to customers, clients, and counterparties. Although, at present, this is only an emerging regulatory requirement in the UK, we see this perspective gaining some traction in recent EU and US regulatory work. This approach may be better suited to helping firms maintain their resilience during extreme events, especially where the alternative delivery of a service is equally as important as the protection of a critical asset, as was seen in the early stages of COVID-19.

- **Strengthen understanding of process dependencies:** where an important business service is identified, firms need a comprehensive map of the systems and processes that support the delivery of that service. This exercise should help firms understand better where the main vulnerabilities in service delivery lie and where they should target additional controls, defences, and invest in redundancies or other forms of substitutability.

### Action for public authorities:

- **Develop macro-operational oversight group:** with increasing digital adoption and IT systems dependencies it is becoming more important for financial regulators to have a unified framework to assess and respond to key operational resilience threats to the sector, similar to how macro-prudential regulators address sector-wide financial risks. This 'macro-operational' oversight can be carried out by the macroprudential regulator, as it is with the FPC in the UK, but should have sufficient authority to conduct air-traffic-control between regulatory bodies to ensure a concerted approach is taken to address the most important threats. Existing authorities in some jurisdictions, such as EU authorities, may currently lack the mandate and powers to carry out such a role effectively.

- **Develop a supervisory approach to third party providers:** if TPPs, such as CSPs, are increasingly seen as critical market infrastructures, then financial regulators need to develop a sustainable approach to regulating their activity in financial services. The EU's DORF may take the lead in developing such an approach, but all jurisdictions need to overcome the challenges of whether to regulate TPPs directly and, if they do, how they will identify which of their functions to regulate. An additional challenge is how a national regulator will approach authorisation/certification of a TPP, especially if it is not headquartered in its jurisdiction.

## Understanding impact

**Actions for firms:**

- **Identify stakeholders and articulate potential harm:** firms should clearly catalogue the stakeholders that could be harmed by an operational event that compromises the confidentiality, availability or integrity of their important business services and the extent of that harm. This exercise should consider harm from the point of view of multiple regulators, including those focused on conduct, prudential soundness and financial stability.
- **Determine if current measures are proportionate to risks and harm:** firms should seek to understand whether their existing operational resilience planning and investment activity are sufficient and targeted enough to match the harm a failure could cause to stakeholders identified by the previous action. This better understanding should also help firms anticipate scrutiny from conduct, prudential and financial stability regulators.

**Action for public authorities:**

- **Deepen work on potentially systemic operational events:** regulators and other public authorities need to lead the sector's thinking on the potential for operational events to trigger systemic financial risk in the financial sector. Early work by the ESRB and the Federal Reserve Bank of New York[xxii] has started the debate on this critical issue, but regulators will need to go further if they are to develop a broader understanding of the most important operational vulnerabilities in the system and the key conduits that could amplify risks and threaten the sector's stability during a disruption.

## Setting tolerance

**Actions for firms:**

- **Articulate risk tolerance for service degradation:** firms should clearly set out their tolerance for the degradation of their important business services during an operational disruption in order to understand better the level of investment needed to meet this tolerance. This should go beyond recovery time objectives and other BAU-type continuity planning measures and instead provide a statement of how many services could tolerably be reduced during a much more severe event.
- **Prioritise the recovery of key business services:** complementing their work on risk tolerance, firms should use their stronger understanding of stakeholder harm to prioritise the services they must restore most urgently following a failure. This will serve as a guide for where the firms needs to invest in service substitutes and alternative methods of delivery in order to maintain the desired level of resilience.

**Action for public authorities:**

- **Align regulatory views on key risks and priorities:** regulators should seek to provide firms with consistent guidance on what their priority areas are for strengthening operational resilience. At a jurisdictional-level, this means strong inter-agency coordination on standards, supervisory practices and scrutiny of firms' investment decisions.
- **Facilitate burden-sharing recovery methods:** regulators should support, and if need be encourage, the development of sector-wide recovery tools such as safe harbouring and other data vaulting programmes in order to strengthen the sector's resilience to data integrity events. The FS-ISAC Sheltered Harbor scheme in the US is the most advanced such programme, and regulators in the UK and EU need to make quick progress to facilitate an equivalent for British and European firms.

## Incident coordination

**Actions for firms:**

- **Cross-sector threat intelligence information sharing:** financial sector firms need to deploy more effective protocols for sharing information about threat intelligence, especially between functional experts in working-level teams. The ECB's expectation that FMIs with an advanced level of cyber maturity develop a partially automated cross-sector intelligence sharing system should ideally be an objective for all financial services firms.

**Action for public authorities:**

- **Strengthen and broaden cross-market groups:** regulators have a key role to play in convening and facilitating collaboration between financial sector firms. This is well developed in the US and is also relatively mature in the UK. The EU, however, only does this for FMIs through the ECB's Euro Area Cyber Resilience Board. EU regulators should seek to develop a similar EU or Eurozone-wide sectoral resilience group for banks and other firms.

- **Facilitate cross-border sharing of leading practice:** threat intelligence sharing across borders is particularly difficult, but authorities should nevertheless seek to facilitate the sharing of leading practices to respond to cross-border threats. The G7's 2019 global cyber incident simulation exercise should be repeated regularly in order to help develop channels for this collaboration.

## Testing

**Actions for firms:**

- **Develop service recovery scenario testing:** whether as part of an explicit requirement or through normal supervisory scrutiny, firms will increasingly need to demonstrate to their regulators that they can maintain important business services during an operational failure. Since most existing types of cyber penetration testing or sector simulations cannot show these capabilities, firms will need to develop, possibly through industry associations, a robust approach to service recovery scenario testing that can convince regulators that investments made in operational resilience have led to actual improvements.

**Action for public authorities:**

- **Further embed penetration testing:** red-team testing should be a core part of the toolkit for supervising important financial services firms. This is already well developed in the UK and US, but regulators in both jurisdictions, and especially in the US, need to take further steps to increase the frequency and consistency of testing firms are required to do. The EU has further to go, and looks set to put clear requirements in place through the DORF proposal. The EU also has the ability to pioneer the cross-border recognition of red-team testing done in other jurisdictions through building on the ECB's existing TIBER-EU recognition mechanism.

- **Develop cross-sector simulation exercises:** The EU presently lacks a cross-sector incident simulation framework for financial services. The ECB coordinates exercises for FMIs (most recently with UNITAS 18[xxiii]), but future cross-border exercises should include banks, insurers, asset managers and other firms. This cross-sectoral approach should mirror that taken by the UK with its SIMEX exercises[xxiv] and in the US with SIFMA's Quantum Dawn series exercises.

Many of these steps may be difficult to achieve, either due to their costs, technical or legal complexity, or the existing level of cooperation between firms or between countries. That said almost every step we recommend in this report has already been put into practice by at least one jurisdiction, authority or industry in our sample. So, while our recommendations may appear ambitious, they are in our view realistically achievable.

### A time for action

Regulators and the senior leaders of financial services firms are increasingly recognising that investing a significant amount of resource and effort into strengthening the operational resilience of the financial sector is now needed in order to reduce the risk of critical failures of resilience, and the operational, reputational and financial consequences that could come with them.

As discussed earlier in the report, some areas of operational resilience, such as cyber risk management, have already shown that the private sector can take a leading role in developing the most innovative and effective solutions to the threats and vulnerabilities that firms face today. It is now time for the financial services sector to take a leading role in more areas of operational resilience, and to develop, insofar as possible, globally consistent approaches that will help financial services groups build and maintain the resilience of their services, wherever they are located.

# Endnotes

i. At the time of writing, guidelines that have been proposed but not finalised by international standard-setting bodies for financial services firms include the Basel Committee on Banking Supervision's principles for operational resilience, and the Financial Stability Board's effective practices for cyber incident response and recovery.

ii. European Supervisory Authorities, Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, April 2019.

iii. European Central Bank, Cyber resilience oversight expectations for financial market infrastructures, December 2019.

iv. European Banking Authority, Guidelines on ICT and security risk management, November 2019.

v. European Insurance and Occupational Pensions Authority, Consultation on guidelines on ICT security and governance, December 2019.

vi. European Central Bank, TIBER-EU framework: how to implement the European framework for Threat Intelligence-based Ethical Red Teaming, May 2018.

vii. European Central Bank, Protecting the European financial sector: the Cyber Information and Intelligence Sharing Initiative, speech by Fabio Panetta, February 2020.

viii. European Systemic Risk Board, Systemic cyber risk, February 2020.

ix. Bank of England, Operational Resilience: Impact tolerances for important business services, consultation paper, December 2019.

x. Bank of England, Cyber in context, speech by Andrew Gracie, July 2015.

xi. UK Finance, Promoting a more cyber resilient culture across financial services, July 2018.

xii. Bank of England, Strengthening individual accountability in banking, Supervisory Statement, February 2020.

xiii. House of Commons Treasury Committee, IT failures in the Financial Services Sector, October 2019.

xiv. Federal Financial Institutions Examination Council, Business Continuity Management, Handbook.

xv. Financial Services Sector Coordinating Council, Business Services Resilience and Restoration: Building Operationally Resilient Business Services in the Financial Sector, April 2019.

xvi. Securities and Exchange Commission, Cybersecurity and Resiliency Observations.

xvii. Greg Baer and Rob Hunter, A Tower of Babel: Cyber Regulation for Financial Services, The Clearing House, 2017.

xviii. Federal Reserve Bank of New York, Thoughts on Cybersecurity from a Supervisory Perspective, speed by Kevin J. Stiroh, Executive Vice President of the NY Fed, April 2019.

xix. Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Joint Statement on Heightened Cybersecurity Risk, January 2020.

xx. Sheltered Harbor, How it works, website.

xxi. Financial Services Information Sharing and Analysis Centre, Exercises Overview.

xxii. Securities Industry and Financial Markets Association, Cybersecurity Exercise: Quantum Dawn V, 2019.

xxiii. Federal Reserve Bank of New York, Cyber Risk and the U.S. Financial System A Pre-Mortem Analysis, Staff Reports, January 2020.

xxiv. European Central Bank, UNITAS Crisis communication exercise report, December 2018.

xxv. Bank of England, Sector Simulation Exercise: SIMEX 2018 Report, September 2019.

# Contacts

If you have any questions about the issues covered in this report, get in touch with one of the team from the Centre for Regulatory Strategy or with one of Deloitte's operational resilience or cyber risk experts.


**David Strachan**
**Partner**
Head of EMEA Centre for Regulatory Strategy
+44 20 7303 4791
dastrachan@deloitte.co.uk

**Rick Cudworth**
**Partner**
Reputation, Crisis & Resilience
+44 7303 4760
rcudworth@deloitte.co.uk

**Nick Seaver**
**Partner**
FS Lead, Cyber Risk Services
+44 20 7303 7097
nseaver@deloitte.co.uk

**Sarah Black**
**Partner**
Risk Advisory
+44 20 7007 9543
sarahblack@deloitte.co.uk

**Irena Gecas-McCarthy**
**Principal**
FSI Director, Deloitte Center for Regulatory Strategy, Americas
+1 212 436 5316
igecasmccarthy@deloitte.com

**Damian Walch**
**Managing Director**
Deloitte US, Risk & Financial Advisory
+1 312 486 4123
dwalch@deloitte.com

**Simon Brennan**
**Director**
EMEA Centre for Regulatory Strategy
+44 20 7303 5267
simbrennan@deloitte.co.uk

**Neil Bourke**
**Director**
Reputation, Crisis & Resilience
+44 20 7303 4682
nebourke@deloitte.co.uk

**Scott Martin**
**Senior Manager, report author**
EMEA Centre for Regulatory Strategy
+44 20 7303 8132
scomartin@deloitte.co.uk

**Quentin Mosseray**
**Assistant Manager**
EMEA Centre for Regulatory Strategy
+44 20 7007 3213
qmosseray@deloitte.co.uk

CENTRE *for*
**REGULATORY STRATEGY**
**EMEA**

The Deloitte Centre for Regulatory Strategy is a powerful resource of information and insight, designed to assist financial institutions manage the complexity and convergence of rapidly increasing new regulation.

With regional hubs in the Americas, Asia Pacific and EMEA, the Centre combines the strength of Deloitte's regional and international network of experienced risk, regulatory, and industry professionals – including a deep roster of former regulators, industry specialists, and business advisers – with a rich understanding of the impact of regulations on business models and strategy.

Deloitte.



Designed by CoRe Creative Services. RITM0527777