UK FINANCE

PERSPECTIVES

Operational resilience in financial services

June 2019

EY
Building a better working world

UK Finance

UK Finance is the collective voice for the banking and finance industry.

Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

Contacts

Andrew Rogan
Director, Capital Markets & Wholesale Policy
Andrew.Rogan@ukfinance.org.uk

Nicholas Edge
Principal, Prudential and Foreign Banks Policy
Nicholas.Edge@ukfinance.org.uk

EY – Financial Services

When the financial services industry works well, it creates growth, prosperity and peace of mind for hundreds of millions of people. No other industry touches so many lives or shapes so many futures.

At EY Financial Services, we share a single focus — to build a better financial services industry, not just for now, but for the future.

We train and nurture inclusive teams to develop minds that can transform, shape and innovate financial services. EY professionals come together from different backgrounds and walks of life to apply their skills and insights to ask better questions. It's these better questions that lead to better answers, benefitting EY clients, their clients and the wider community. Our minds are made to protect a better financial services industry. It's how we play our part in building a better working world.

ey.com/ukfs

Contacts

Ali Kazmi, Partner, Ernst & Young LLP
AKazmi@uk.ey.com

Chris Richardson, Partner, Ernst & Young LLP
crichardson4@uk.ey.com

Jason Mclean, Partner, Ernst & Young LLP
Jason.Mclean@uk.ey.com

Steve Holt, Partner Ernst & Young LLP
sholt2@uk.ey.com

TABLE OF CONTENTS

Introduction to operational resilience 2

Executive summary 4

Achieving operational resilience – the regulatory story so far, and what's to come 6

Achieving operational resilience – industry challenges and perspectives for consideration 10

Practical next steps 26

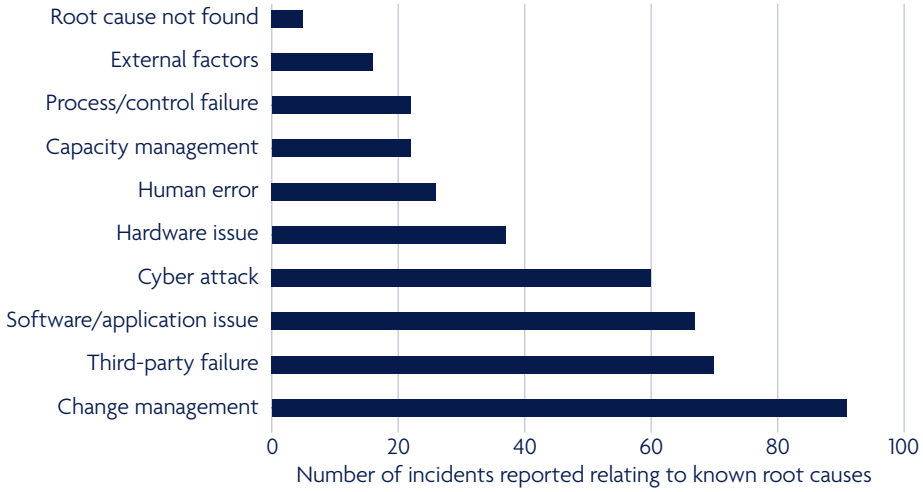
Contributors 28

Introduction to operational resilience

Operational resilience in UK financial services is defined as the "ability of firms, financial market infrastructures (FMIs) and the system as a whole to prevent, adapt and respond to, and recover and learn from, operational disruption". [1]

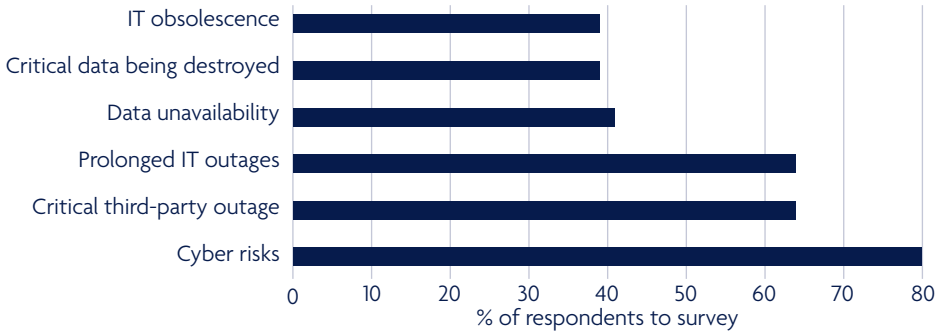
Achieving operational resilience requires a firm not only to focus on minimising the likelihood of an incident occurring and causing a disruption, but also to assume that disruptions do occur and put robust response and recovery processes in place. Disruption comes from a variety of sources, as demonstrated by the Financial Conduct Authority's (FCA) analysis of technology and cyber resilience in 2018:

Figure 1 Root causes reported to the FCA, October 2017 – September 2018 [2]



These results are complemented by the ninth annual *EY/IIF* global bank risk management survey,[3] which identified the following top resilience concerns for respondents:

Figure 2 Top resilience concerns for bank risk functions



1. FCA, PRA, BoE, Building the UK financial sector's operational resilience, July 2018.
2. https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf. (
3. Ninth annual global bank risk management survey, Accelerating digital transformation, EY/IIF, 2018.

As these results indicate, achieving resilience in a complex environment requires the coordination and cooperation of many existing capabilities within a firm. These include, but are not limited to: operational risk management (including change management and third-party management), risk ownership in the business, operations management and technology risk management (including, business continuity management, disaster recovery, information security and data privacy).

Regulators and other stakeholders are taking an increasingly proactive role in challenging the operational resilience of firms in the financial sector. Firms are also facing increased internal and external threats and vulnerabilities, increasing pace of change, existential cyber threat, and vastly complex supply chains. Therefore, it is vital that firms take a broad view on enhancing their operational resilience capabilities.

PURPOSE OF THIS PAPER

Following the publication of the joint discussion paper *Building the UK financial sector's operational resilience*[4] in July 2018 ("the Joint Discussion Paper") by the Bank of England, Prudential Regulatory Authority and FCA, UK Finance, in partnership with EY, held a number of workshops with members representing a range of retail, commercial, custody and wholesale financial institutions.

These workshops brought together representatives from across UK Finance's membership to discuss a range of areas which we touch upon within this paper. Our aim is not to prescribe a specific approach or gold standard but to offer perspectives to help inform the industry. These perspectives may be useful to individual firms as they look to enhance their own resilience as well as contribute to the greater resilience of the sector.

The perspectives set out in this white paper are the synthesis of UK Finance workshops and EY's discussions with more than 70 firms on their resilience concerns, current activities and planned enhancements.

UK Finance and EY hope that the thoughts shared within this paper help equip firms to evolve their approach to resilience in a proportionate manner.

4. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

EXECUTIVE SUMMARY

There is undoubtedly significant and increasing focus on enhancing the operational resilience of both individual firms and the wider financial sector. Members recognise that achieving operational resilience is not just a regulatory compliance issue but a business imperative. Building and maintaining trust with consumers and businesses is an integral part of the financial services system, which benefits firms, their customers, clients, shareholders and the wider economy. Continuity of service across the sector is a key element in protecting society and is a strategic consideration up to Board level.

Industry has been focusing on enhancing resilience for a number of years, moving the emphasis from primarily technology solutions to adopting a broader business-led approach.

In response to the principles set out in the joint discussion paper firms are challenging their existing approaches. In doing so firms are considering what further enhancements of their operational resilience "means for them".

Based on discussions with UK Finance members and input from EY, a summary of the key activities that firms are undertaking include:

- Identifying their most important business services
- Exploring mechanisms for setting impact tolerances
- Performing a gap assessment of their current approach against evolving consumer and market expectations

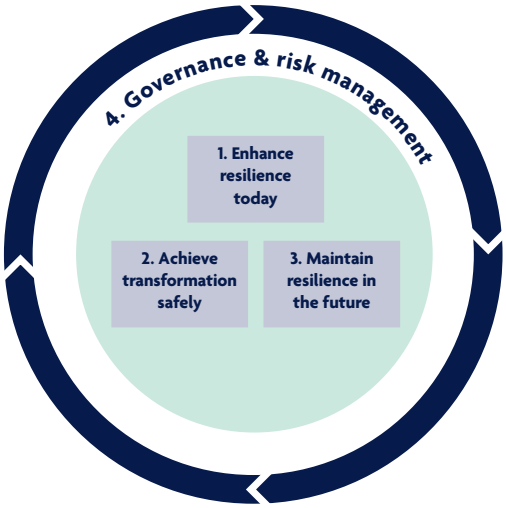
These activities lay the foundation to developing a response that evolves their existing approach to managing risk and achieving resilience but is proportionate to the services they provide, how consumers and markets rely on them, and the role they play in the sector.

Challenges undoubtedly remain. Whilst UK regulators' supervisory approach remains under development, and the timeline for implementation is currently unclear. Whilst the principles set out in the discussion paper are acknowledged by the industry, the practicalities of how individual firms can meet the needs of their customers and clients in this context remains an area of significant discussion, effort and focus. These challenges are compounded by the need for operational resilience to compete with other strategic considerations and risk drivers, including Brexit, technology change and competitive market needs.

Members recognise that to achieve a robust and operationally resilient organisation requires a coordinated and broad range of activities linked to risk, regulatory and strategic drivers. Reflecting on member feedback it is clear several groupings of activities are emerging that will move the needle, these are:

1. Enhance resilience today.
2. Achieve transformation safely.
3. Maintain resilience in the future.
4. Gain oversight through robust governance and enhanced risk management.

Figure 3: Strategic operational resilience model



Enhancing resilience today draws most firms' current focus, taking the principles derived from best practice and emphasised by regulators. Key activities include:

1. Identifying the most important business services and setting impact tolerances.
2. Assessing prevention, response and recovery capabilities against resilience expectations and remediating gaps where appropriate.
3. Increasing focus on understanding and managing the risks posed by third parties.

Achieving transformation safely is emerging as another focus areas. As firms seek to reduce complexity, deliver enhanced technology platforms, and innovate in the way that they serve consumers and markets, many firms are recognising that they should:

1. Build resilience considerations 'by design' into the platforms, products and operating models of the future.
2. Enhance the way that risk is managed through the delivery life cycle and ensuring governance is robust.
3. Assure delivery through enhanced testing and validation of solutions prior to going live.

Maintain resilience in the future this requires focus on resilience in the holistic sense when defining 'to be' target operating models, products and services. Key considerations include:

1. Not losing sight of 'operational' resilience in the context of the enhanced technology resilience capabilities offered by the cloud, automation and big data, and developing solutions that can adapt to disruption.
2. The need for better access to data and enhanced management information (MI), and to unlock the power of continuous monitoring and risk management to better inform decision-making across the firm.

Oversight through robust governance and enhanced risk management will underpin each of the 'stages' of resilience set out above. After all, operational resilience is commonly understood to be the outcome of effective management of operational risks. Key activities include:

1. Balancing the achievement of resilience with other drivers, which requires constant vigilance and challenge by boards and senior management.
2. Recognising that resilience is a dynamic concept and embedding a mindset of continuous monitoring and improvement throughout the organisational approach.
3. Ensuring flexibility, as well as proactive engagement by and with regulators, to demonstrate that there is not a single path to enhanced risk and resilience management.

The pages that follow set out the regulatory story where we have come from and where we are going, as well as our perspectives from industry engagement and workshops with members. Finally, we set out ten practical steps that firms can take to structure their journey to enhanced operational resilience today.

Achieving operational resilience – the regulatory story so far, and what's to come

To make sure that we fully appreciate the regulatory direction of travel regarding enhancing operational resilience, it is worth spending a moment reflecting on the journey so far. As set out in the timeline on page eight, regulatory attention on operational resilience did not start in 2018 with the publication of the Joint Discussion Paper *Building the UK financial sector's operational resilience*.[5]

ORIGINS OF THE REGULATORY APPROACH TO OPERATIONAL RESILIENCE

Enhancing firms' management of operational risk was brought into sharper focus by events such as those of 11 September 2001 and the increasing attention on sector-wide disruption and the importance of data recoverability. In the intervening years, the global financial crisis brought financial resilience up the agenda. Following high-profile outages and the first 'Dear Chairman exercise' on operational resilience in 2012, the bar continued to rise steadily with increasing pace.

Innovative changes in the way that financial services are being delivered and the associated risks of wider adoption of evolving technologies into customer channels raises the profile of non-financial risk. Regulatory attention has been drawn to the need to adapt to the new operational approaches and focus has shifted towards ensuring that financial institutions can continuously deliver services to customers and markets through shocks and disruptions.

The UK regulators' expectation is that operational resilience should be considered on a par with financial resilience by boards, executive management and firms as a whole. An additional challenge for all parts of the industry is managing the significant level of mandated regulatory change currently facing the sector. The potential impact of this on the resilience on the sector is an important consideration for industry, regulators and government.

However, regulatory focus is not the only driver sharpening minds, given changing consumer expectations, pace of change and digitisation.

5. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

WHAT'S NEXT?

Following on from the 2018 Joint Discussion Paper, the authorities are already expecting firms to be seriously considering the principles it sets out. This is demonstrated through ongoing supervisory engagements across the sector and the PRA's request for some firms' internal audit functions to review their current approach.

The existing PRA rulebook and the FCA handbook are likely to contain the majority of the baseline regulatory requirements; for example, the Senior Management Arrangements, Systems and Controls (SYSC) eight principles for managing outsourcing risk. Going forward, additional clarifications on how operational resilience will be embedded into the supervisory framework are expected.

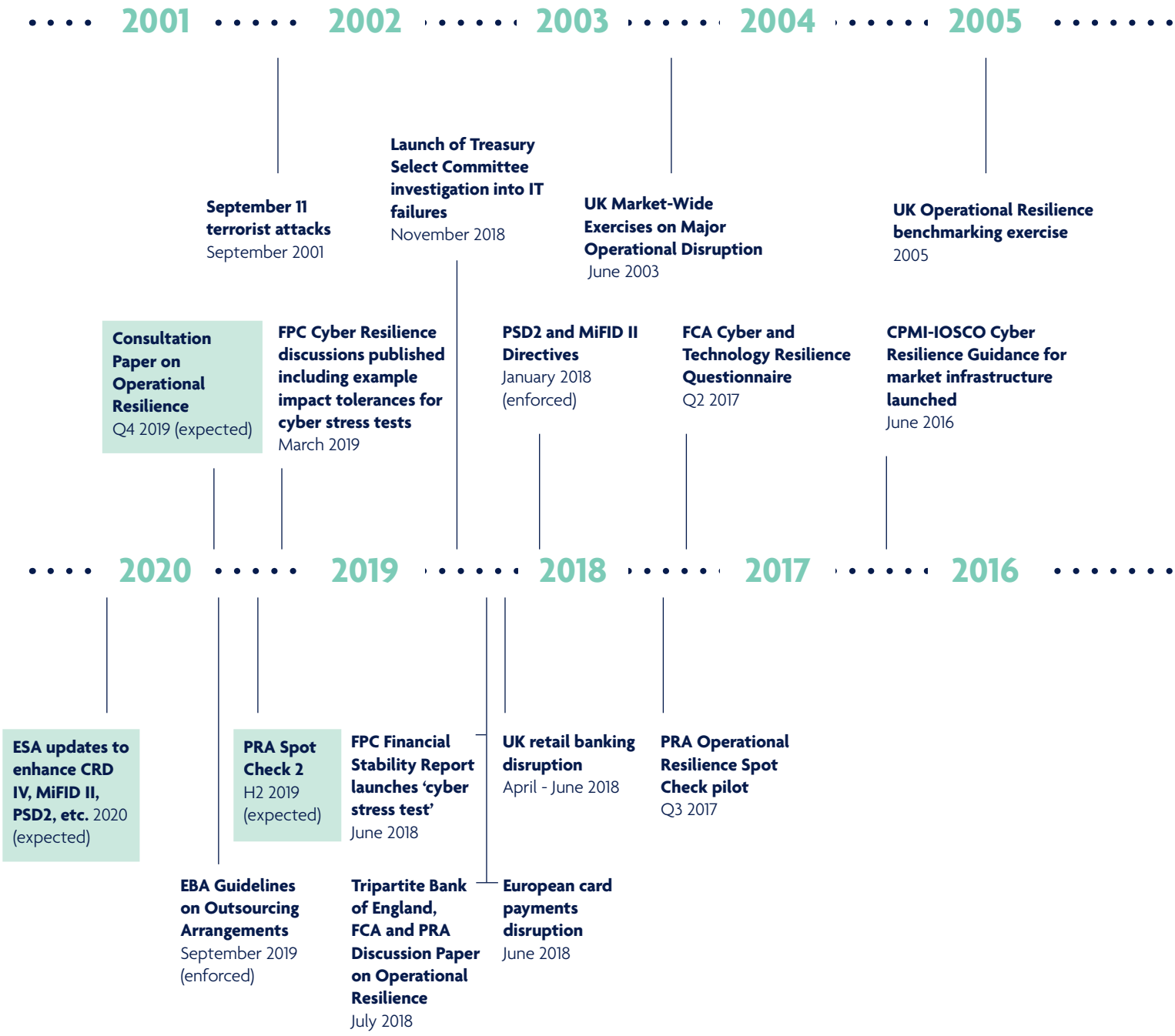
The discussion paper advocates a more holistic and business-led approach to resilience, which should enable improved investment decisions at board level. Industry will also be factoring in the use of the Senior Manager Function 24 (SMF24 - Operations) in determining the most appropriate way to gain organisational oversight. The industry is looking forward to seeing how the authorities are furthering their views in the consultation paper, which is expected in Q4 2019.

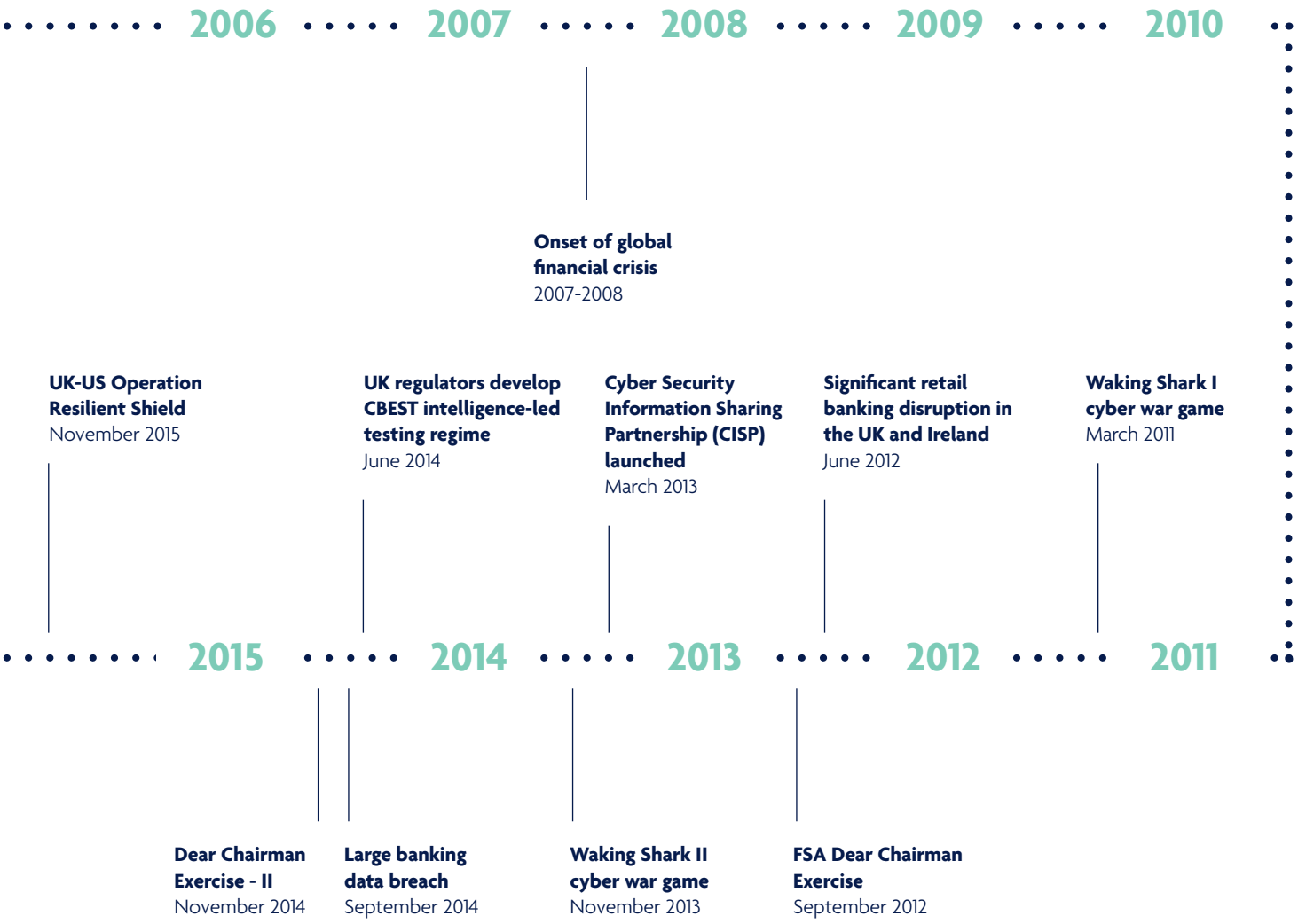
In addition to the UK authorities releasing their paper, we are seeing resilience become a core focus across the EU, the US and further afield. Currently, the European Commission and the European supervisory authorities are looking at updating existing requirements, such as CRD, Solvency, and PSD regulations, to add more focus on resilience issues, including operational and cyber risk.[6]

For example, the Payments Services Regulation (PSR) Regulation 98 already sets out a vision for proactive risk and resilience management, including continuous monitoring, which looks likely to be followed up in forthcoming EBA Information and Communication Technology (ICT) guidelines. Outside the EU, we have seen global regulatory focus starting to turn to operational resilience; for example, with the Basel Committee establishing an Operational Resilience Working Group and US regulators mandating remediation activity relating to resilience.

6. https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

TIMELINE OF SIGNIFICANT OPERATIONAL RESILIENCE EVENTS




2006
2007
2008
2009
2010
2015
2014
2013
2012
2011
Onset of global financial crisis
2007-2008
UK-US Operation Resilient Shield
November 2015
UK regulators develop CBEST intelligence-led testing regime
June 2014
Cyber Security Information Sharing Partnership (CISP) launched
March 2013
Significant retail banking disruption in the UK and Ireland
June 2012
Waking Shark I cyber war game
March 2011
Dear Chairman Exercise - II
November 2014
Large banking data breach
September 2014
Waking Shark II cyber war game
November 2013
FSA Dear Chairman Exercise
September 2012

Achieving operational resilience – industry challenges and perspectives for consideration

Over time, there will be a need to harmonise disparate regulatory requirements in order to achieve effective operational resilience, particularly for organisations that operate in multiple jurisdictions globally.

This will be an evolution, not a revolution, building upon existing capabilities within firms and the sector while recognising the improvements that have already been made. That being said, there is a need to recognise that this is a significant change in focus and intent of the authorities. Firms will need to take proactive steps in order to meet changing regulatory and customer expectations.

Whilst not an exhaustive list, the following areas have been identified as helpful to focus on as firms look to enhance their operational resilience:

1. Role of the board
2. Strategy, governance and MI for operational resilience
3. Identifying and understanding the most important business services
4. Setting and testing against impact tolerances
5. Integration into the risk management framework
6. Resilience through change and transformation
7. Testing and exercising
8. Communication

1. THE BOARD

The challenge

There is a heavy regulatory emphasis on the role of the board in achieving operational resilience. Organisational direction and strategy starts at the top, and the July 2018 Joint Discussion Paper explicitly calls on firms' boards to be actively involved in challenging management's definition of the most important business services and impact tolerances, and overseeing the organisational framework and performance more broadly.

The breadth of risks to resilience and the range of capabilities required to be aligned to respond to them across the enterprise pose a significant challenge to effective oversight. Organisational complexity, the pace of change and unpredictability of external threats are all factors that make it difficult for boards and senior management to read across an enterprise and identify areas to focus on.

Expectations of the board have been cemented by recent regulatory focus on operational resilience oversight and reporting. Senior management have increasingly been challenged by non-executive directors (NEDs) on the robustness of their approach to achieving resilience. Many firms are struggling to articulate the role of the board, and to educate and fully involve it in establishing an organisational approach which has historically been driven from the bottom-up.

Firms highlighted that operational resilience has to compete with other significant investment, regulatory and risk issues on the board agenda. There is also a tension identified between legal entity and group for complex or global organisations given the cross-jurisdictional nature of many services and the (public) mismatch in regulatory expectations.

Perspectives to consider

Members of the UK Finance operational resilience working groups reported varying degrees of board involvement in their firm's operational resilience frameworks.

Role of the board

There are a number of approaches that members have taken when considering the role of the board. Firms have varyingly reported that resilience might be a standing agenda item for the full board, focused on primarily by the board risk committee, or the topic of a specific committee of the board.

The availability of relevant skills and experience on the board is a consistent theme in the industry. Some firms identified a specific non-executive member of the board responsible for challenge and oversight of resilience issues as part of a board committee, with the topic making up a significant part of the agenda. Generally, this individual has had relevant experience in technology, risk or operations to enable them to challenge management effectively. More broadly, firms are also focusing on training and awareness for board members on operational resilience, similar to the exercises run for other regulatory focus areas such as conduct and cyber.

Some members indicated that their boards are involved in overseeing the alignment of the operational resilience strategy with the firm-wide strategy. Many firms are involving the board in the review and validation of both the methodology and output for defining the most important business services and impact tolerances, as well as relevant risk appetites, which allows for improved decision-making. Boards are also considered critical to reviewing, challenging and, ultimately, approving an integrated, firm-wide resilience operating model.

Board-level oversight of change programmes and associated risks to consumers, operational stability and security was also high on the agenda for many firms. Finally, the role of the board during an incident was an area of focus for firms that had experienced significant disruptions. This echoes recent public and non-public examples of major disruption in financial services.

Reporting to the board

Reporting to the board should be actionable and understandable, and include information on significant initiatives, investments, regulatory focus areas and emerging risk themes. Like other topics, boards should receive information that is an aggregation of the layered reporting established through the firm. The aim is to provide insights that address resilience holistically and enable informed investment decision-making or risk acceptance at the highest level.

Frequency of reporting currently varies from monthly to every six months, depending on the appetite of the board for receipt of resilience metrics and insights. This issue is an ongoing area of discussion for many firms with views still evolving.

Many firms are currently struggling to find a balance between 'positive assurance' and providing too much detail to the board, and reporting by exception. Dashboards are being defined to demonstrate not only the performance of the overall resilience framework and key capabilities, but also the resilience of the most important services and the performance against impact tolerances and risk appetites.

Where aggregated metrics or dashboards are presented, it is crucial that these are aligned to criticality, tolerances and risk appetite and that there is robust challenge to the supporting metrics. Given core elements of the resilience framework will require re-evaluation as consumer behaviour, market forces and broader systemic resilience considerations evolve, dashboards and reporting will need to be equally dynamic.

Key questions to consider:

1. To what extent is the board involved in setting or validating the firm-wide resilience strategy?
2. How does the board oversee resilience and does the information they are provided enable decision-making for investment or risk acceptance as appropriate?
3. How confident is your firm that the role of the board during a period of disruption is clear and well tested?
4. Does your board feel well informed on your current operational resilience arrangements?

2. STRATEGY, GOVERNANCE AND MI

The challenge

Operational resilience has not traditionally been an explicit consideration in most organisations' business strategy. However, in recent years many firms have increasingly identified business benefits in achieving resilience individually, and for the system as a whole.

Like financial resilience, the industry needs to ensure that operational resilience as an outcome is managed in order to help ensure that the financial system is able to absorb operational shocks, as well as financial shocks, and continue to provide important business services, both in a benign environment and during times of stress.

Achieving operational resilience requires the alignment of a range of existing capabilities and refocusing of governance and risk management activities. The complexity of aligning these capabilities is compounded by current organisational factors such as global footprints, diverse reporting lines and silos. This is most challenging when reconciling existing divisional governance with accountability for end-to-end business services.

Existing management information and reporting for continuity and recovery capabilities is often not aligned to a business service view. Metrics are often process driven rather than giving management a clear answer to the question 'How resilient are we?'

Perspectives to consider

Strategy

Firms need to develop firm-wide operational resilience strategy and operating models that are aligned to both enterprise strategy and risk appetite. This is to help ensure that key components of resilience are aligned with a core aim and vision depending on the risk posed to important business services. Once formed, the resilience strategy should be reviewed with senior stakeholders, including the board.

Some firms are also focused on embedding resilience considerations into broader organisational strategy, including the design of future operating models and ways of delivering services at the earliest possible stage. This makes sense as it will help firms better maintain resilience in the future. It is also commensurate with the board and regulatory imperative to ensure that investment decisions and risk acceptances are considered holistically and aligned with resilience considerations.

Strategy should be underpinned by a framework that clearly articulates key activities, processes, roles and responsibilities that enable operational resilience across the organisation. An operational resilience outcome should integrate with existing frameworks and clearly set expectations for how resilience will be built into existing capabilities.

Governance

Senior management should take responsibility for owning the operational resilience strategy, framework- most important business services, key resilience capabilities and, ultimately, set an appropriate 'tone from the top'. By taking a holistic approach to how business services are provided to the firm's customers and understanding the underpinning capabilities that support them, senior management will be able to highlight areas of potential weakness and address them appropriately through investment.

In our experience, firms are still working through the appropriate governance mechanisms for business services that span many jurisdictions and teams across the globe. No standardised models are forming, but organisations are considering (documented) delegation of responsibility beyond the SMF24 and using resilience governance forums as some of the mechanisms to make resilience a reality.

Roles should be defined within the business, operations and technology for resilience and should also be embedded across the three lines of defence. First-line senior management owns and manages risks to resilience, and should be challenged by the second-line. Internal audit has an important role to play in challenging the governance framework and giving assurance over key resilience capabilities.

Management Information (MI)

Many firms are currently focused on shaping what MI should be provided to key decision makers at various levels in the organisation.

Three 'dimensions' of reporting have been identified by participants in UK Finance working groups that might be considered by firms:

1. Service-view resilience reporting, providing responsible owners with oversight of the robustness of the firm's most important business services with reference to impact tolerances and risk appetites
2. Capability-view resilience reporting, providing a thematic assessment of the resilience of technology, third party, people, processes and property components supporting important business services
3. Holistic reporting on the maturity of the resilience operating model and framework, and the operation of cross-cutting functions such as business continuity management, disaster recovery, incident management and cyber controls

A firm-wide approach to measuring and reporting on resilience should be holistic, aligned to the risk framework and provide actionable information to the right stakeholders at the right time.

Firms taking part in our workshops have been considering the extent to which senior management will be provided with positive assurance or exception-based reporting. This is clearly a consideration that should be based on the preferences of the senior leaders receiving the data. However, some firms are working on the principle that they will provide more data to senior management in the early stages of their operational resilience programme, and adjust accordingly to reflect the maturing of the organisational approach over time.

Actionable, timely management information should enable more informed decision-making on investments and risk acceptance, as appropriate.

Key questions to ask:

1. Does your resilience framework have the support of the business and are roles and responsibilities clear from the board and executive leadership down?
2. Are your business lines demonstrating ownership, leadership and accountability for resilience?
3. Is your firm-wide approach to measuring and reporting on resilience holistic aligned to the risk framework and does it provide actionable information to the right stakeholders at the right time?

3. IDENTIFYING AND UNDERSTANDING THE MOST IMPORTANT BUSINESS SERVICES

The challenge

One of the challenges in complying with future regulatory expectations is the risk of inconsistency in firms' identification of the 'most important business services' given the lack of clear guidance on how to apply the principle.

Perspectives to consider

Defining the most important business services

The most important business services should be identified through a repeatable methodology, with demonstrable logic. The approach should start from a list of core business services that the organisation provides to consumers, rather than from a list of supporting processes, third parties or systems that are identified as 'critical'. It is expected that this list of services will be broader than those defined as 'critical economic functions' used in recovery and resolution planning activities.

Working top-down rather than bottom-up will identify core business services that are provided to customers and how they can be influenced by external and internal factors, which can then be mapped and tested logically to build on firms' existing frameworks.

A robust methodology for identifying the most important business services should be applied, which can be explained to boards, senior management, regulators and other stakeholders.

The assessment should consider the impact on internal processes, stakeholders and performance of disruption, and be undertaken in parallel with assessment of the potential impact on customers, markets, third parties and business partners.

This assessment might also consider the broader ecosystem impact of disruption to those that the firm does not directly contract with or provide services to. Whilst services identified will be individual to each, firms might find it helpful to consider potential impacts on the authorities' objectives around promoting safety and soundness of firms, focusing on the harm they can cause to the stability of the UK financial system, as well as ensuring relevant markets function well.

Both the methodology for identifying the most important business services and its output should be considered and ratified by senior management and the board.

Determining the population and relative importance of the most important business services can be a complex decision to make, and the outcome is likely to change dynamically over time. Key drivers might include changes in consumer or market behaviours, business strategy, market share or organisational structure through mergers, acquisitions or divestments.

Understanding the most important business services end-to-end

Following the 'map' principle referred to in the Joint Discussion Paper, many firms are undertaking service mapping to identify internal and external dependencies supporting their most important business services.

This involves taking a horizontal view of a service and mapping key components supporting the processes that constitute it to identify technologies, supporting processes, people, facilities, third parties and data that are critical to its operation.

Beyond internal dependencies, reliance on third parties is ever growing, and many firms are focusing not only on direct third parties but also the extended supply chain, including fourth and even fifth parties. [7] Concentration risk in third parties as well as essential infrastructure are significant considerations for many firms' resilience activities and the market as a whole.

Recognising the level of effort required to map internal and external dependencies, many firms are conducting pilots to refine their proposed approach.

In our experience, many larger or more complex firms cannot expect to map a service end-to- end and top- to- bottom from the outset. These firms are, therefore, defining a strategic approach to map to a specific level of depth as a first pass, with future iterations increasing the depth and specificity.

Having mapped dependencies, firms should assess the risks to resilience inherent in the components that support the service. They should also consider these components' and processes' robustness against resilience considerations including the identification of single points of failure, gaps in processes and controls, and robustness of response and recovery capabilities. Risks, vulnerabilities and issues outside appetite should be reported on, treated in line with existing risk management techniques and, ultimately, prioritised for investment or risk acceptance accordingly.

Key questions to ask:

1. To what extent have you identified and ranked your most important business services?
2. To what extent have the board and senior management discussed the list, and do they understand the consequences in terms of prioritising this list over other services?
3. Have end-to-end services been mapped and risk assessed to identify gaps in capabilities and likely 'hot spots'?

7. Please see our recent white paper on Third-Party Risk Management: Keeping control in a rapidly changing world for further insight: https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/third-party-risk-management-keeping-control-rapidly-changing-world.

4. SETTING AND TESTING AGAINST IMPACT TOLERANCES

The challenge

Further complexity arises when firms start to set impact tolerances. Over time these will become a key management lever as they will become inputs to investment decisions, crisis management and a data point for external monitoring of a firm's approach to achieving resilience. The supervisory authorities envisage using impact tolerances as a key data point to use when discussing operational resilience with a firm or peer group of firms.

The level at which a firm (or peer group of firms) sets impact tolerances is inherently linked to the proportionality of its approach to enhancing operational resilience.

Organisations should aim to understand the acceptable level of stress and resilience needed from their most important business services in order to guide investment decision into those areas. One challenge most firms are considering is how to integrate the concept of impact tolerances with existing methods of measuring and monitoring risks to resilience and organisational performance including risk appetites, risk tolerances and risk/issue ratings.

Perspectives to consider

Setting impact tolerances

Firms should consider using an established taxonomy such as confidentiality, integrity and availability to identify a range of potential disruptions to important business services. In doing so, they can identify different potential harms to consumers, market participants and the firm itself that might inform the setting of a tolerance.

The objective is not to identify each possible root cause of such disruption but focus on service-level impact. The objective should be to assess the impact of a disruption agnostic of how the event arose.

Impact tolerances should consider the impact of disruption on internal processes, stakeholders and performance in parallel with assessment of the potential impact on customers, markets, third parties and business partners. This consideration might also include the broader ecosystem impact of disruption to those that the firm does not directly contract with or provide services to.

Tolerances should be measurable and defined as upper limits to be avoided in all but the most extreme scenarios. This might be articulated in the form of a specific outcome or metric combining time, volume and value measures.

Mechanisms should be put in place to review and reassess impact tolerances as the business or operating model changes. Given the emphasis on consumer, client and market impacts on the definition of tolerances, periodic reassessments should be completed to take into account changes in the nature or extent of reliance on a service by its users.

Testing against impact tolerances

Setting tolerances will help enable organisations to drive out tangible activity by assessing resilience capabilities and identifying gaps, influencing escalation during a disruption and aiding the measurement of risk exposure.

Impact tolerances are envisaged to be thresholds that a firm should not breach in any but the most extreme circumstances. As they are a relatively new concept, the industry approach to testing against tolerances is immature.

However, assessing end-to-end adaptive response and recovery capabilities through 'table-top' scenario analysis is a good starting point. Introducing increasingly challenging injects to stress capabilities and assess how a firm or function might cope with severe scenarios is not a new concept for firms who already partake in economic stress testing and cyber 'war gaming'. These techniques can be applied more broadly to help a firm understand how much it would take to breach an impact tolerance and assess whether further remediation or investment is required.

Reporting on performance against impact tolerances is a relatively formative area for most firms. As approaches to testing mature, it is envisaged that the outcome of testing and any actual or simulated breaches of impact tolerances will be reported in a way that aligns to existing reporting on risk appetites and tolerances.

Key questions to ask:

1. Have you determined what you need to sustain each important business service, using whatever means are available to avoid harm to consumers and markets?
2. Are the board and senior management comfortable with these impact tolerances?
3. Have you appropriately tested whether you can, in fact, sustain services for the time, volume and value set out in your impact tolerances?

5. RISK INTEGRATION

The challenge

Operational resilience is an outcome enabled by effective management of risk. As set out in the introduction, operational risk and resilience has not had equal attention from regulators and some firms in comparison with financial risks and resilience over the past ten years. However, a refreshed industry approach to achieving operational resilience is necessitating an evolution of existing operational risk management tools and techniques. Whilst it is important to continue to identify, measure, manage and prevent operational risks crystallising[8], achieving operational resilience requires firms to assume that disruptions will occur as risks crystallise.

Many traditional operational risk methods and risk appetites have focused inwards, considering reputational, financial and regulatory impacts on a firm, rather than broader consumer and ecosystem impacts of disruption. Probability has also been a primary driver when conducting risk assessments, therefore assuming failure provides a new dimension to risk management activities.

Response and recovery capabilities such as incident management and business continuity have always been foundational components of an operational risk framework. The evolving approach to operational resilience highlights the need for these disciplines, and broader risk management techniques, to cut across silos within the organisation and focus on end to end business services, rather than individual teams, systems or facilities.

Perspectives to consider

Sustaining operational resilience will require the integration and embedding of risk frameworks to enhance preventative, responsive, recovery and learning capabilities. Many capabilities required to effectively manage risks to operational resilience are already present in most organisations' enterprise-wide risk management frameworks. This is an evolution rather than a revolution of risk management.

Many firms are considering adapting their risk assessments to look at risk 'front-to-back' which has the potential to align well with a focus on business service. Risks identified through service mapping and stress testing activities are being consolidated with service risk assessments to provide a more holistic risk view.

Risk data is increasingly recognised as a valuable asset to enhancing operational resilience. The aforementioned service mapping outputs and service risk assessments provide a richness of data that can be combined with internal and external sources such as threat intelligence, incident data and loss events.

Firms are starting to harness the power of improved quality and availability of risk and control data from 'as a service' cloud applications and infrastructure. Analytics, including artificial intelligence and machine learning techniques, will increasingly be applied to large data sets to facilitate continuous monitoring of threats and vulnerabilities and enable more data-driven and fact-based risk assessments.

Key questions to ask:

1. To what extent have you coordinated operational resilience activities with your operational risk and enterprise-wide risk management frameworks?
2. What steps would you need to take to enable you to continuously monitor risks to resilience?

8. As was noted by the PRA's Charlotte Gerken in 2017 when setting out thoughts on the Bank of England's approach to operational resilience, see https://www.bankofengland.co.uk/-/media/boe/files/speech/2017/the-boes-approach-to-operational-resilience.pdf

6. RESILIENCE THROUGH TRANSFORMATION AND CHANGE

The challenge

Increasing consumer expectations and competition are putting pressure on firms to be agile and innovative. Advances in new technologies create the potential for a well-established and complex businesses to increase distribution, reach new markets and customers, move to real time capabilities, be better informed to make better decisions and connect with a highly engaged consumer who can be connected to anyone, anywhere at any time.

To meet these demands, businesses across the financial services are investing heavily in new technologies that seek to retire the technology applications and infrastructure that had underpinned the existing or old ways of working.

However, the scale of such a change can bring both long-term advantage and expose the enterprise to many new risks. New technology architectures change the way business and technology services and processes are delivered, introducing new and often unforeseen points of stress or failure to the business.

It is recognised that change is the most prevalent cause of disruption, according to the FCA9, and is a primary focus of its Business Plan 2019/2010. It has also been an area of focus for the Treasury Select Committee (TSC)[11], opening an inquiry into IT failures in the financial services sector.

The design, development, testing and deployment discipline required to safely implement new front-end technologies, core software platforms and supporting middleware, infrastructure, processes and controls is complex and should not be underestimated.

Further, a shift in the technology estate to adopt new and modern technologies can also alter ways of working and the workforce model across the business. These changes can represent a significant shift in how the business operates both in normal operating conditions and in times of stress.

Embedding resilience considerations into the change life cycle should be a co-ordinated, enterprise-wide agenda item. This will have board accountability and oversight implications that will continue to be an ongoing challenge amplified in years to come.

Perspectives to consider

It is imperative that resilience considerations are embedded into transformation and change initiatives. New solutions, products and technology platforms should be rigorously designed, built and tested with resilience in mind, with professionals focused on resilience included in the transformation and change initiative from the start.

Many organisations are defining a strategic road map to enhance resilience through a combination of new technology platforms, migrating to cloud services, engaging in partnerships and embracing enablers such as agile and automation. The impact of these decisions on holistic operational resilience needs to be considered and built in to investment cases.

9. https://www.fca.org.uk/publications/research/cyber-technology-resilience-themes-cross-sector-survey-2017-18)
10. https://www.fca.org.uk/publications/corporate-documents/our-business-plan-2019-20
11. https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/inquiries1/parliament-2017/inquiry1/publications/

The journey towards a more resilient operating model is fraught with delivery and operational risks. Effective oversight starts with the board and should be a focus of the full executive team, rather than just focused on technology – it is a strategic imperative that demands significant attention.

Challenge through the delivery life cycle is important, and key areas of focus include a keen focus on the acceptance of scope changes and enterprise-wide risks. Key controls, escalations and quality leading/lagging indicators need to be embedded through the life cycle of both small change initiatives and enterprise-wide transformations alike, albeit proportionately to the risk posed by the change.

Robust testing is a key quality and completeness indicator that lies at the heart of business and technical readiness. This should at a minimum include stress-testing integration with third parties and partners, functional as well as non-functional coverage of the solution, performance and stability both under 'happy path' and exception-based scenarios.

The role of the second - or third-line - is to challenge operational readiness, the management of dependencies and 'planning for failure' through robust rollback plans, training plans, communication plans both internally and to customers.

Key questions to ask:

1. Do you know what your future architecture and operating model look like and how you will operate in a resilient manner in the meantime?
2. How robust is your oversight and challenge of change?
3. Are your implementation strategy, controls and testing robust enough for both major transformation and business-as-usual change?
4. Once the new technology solution is deployed, do we have robust and appropriate processes, control and MI to deliver the ongoing stability of the technology solution?

7. EXERCISING AND SIMULATIONS

The challenge

Exercising and simulations are a useful way of testing response and recovery capabilities. Firms and the wider industry recognise that a lack of preparedness, slow decision-making and ineffective communications often impede appropriately tackling an incident. Boards and senior management need to be prepared and practiced in responding to major incidents. It's clear that rehearsing through simulation exercises to identify key actions, roles and responsibilities is the best way to prepare for severe stress events, including liquidity, counterparty default and operational failure (e.g., third-party outage, cyber attacks or loss of location).

Some firms overlook the importance of rehearsing time-pressured, technical, process and business decision-making, which are important components of being ready to respond to disruption. Indeed, many firms already have a plethora of crisis or contingency plans, but few have integrated portfolios, simulations or table-top testing strategies that will enable them to respond effectively in a real-life event.

Perspectives to consider

Simulations that are run effectively can help organisations shape connected contingency plans in line with the discussion paper principles; namely, the need for organisations to have a joined-up approach to incident and crisis management, with all relevant stakeholders and interested parties engaged and involved as appropriate.

Simulations are taking place across a variety of areas within a firm. There may be benefits to aligning activities across each of the following:

1. **Financial resilience** – management of financial resources (capital, liquidity and collateral) in severe stress
2. **Business continuity** – ability to deliver business services continuously when people, processes, technology or third parties fail, with links to response and recovery plans
3. **Disaster recovery** – ability of IT to deliver high availability and speed with accurate recovery
4. **Cyber response** – management of cyber crises impacting confidentiality, integrity, and availability of data and processing
5. **Operational Continuity in Resolution (OCIR)** integrity of a firm's resolution plan, with links between the plan and crisis management

Simulations should involve scenarios and complicating factors that help to mimic a real-world incident. For a scenario to be credible, it should include inputs from business, risk management, regulatory, systemic, consumer or client, technology, communication and governance perspectives.

This makes the simulation relevant for individuals across the firm, as well as external stakeholders. Injects should also be realistic, given current real-world threats.

A successful simulation should enable the creation of a response plan that is tailored to the organisation. The response plan should follow a structured approach, including detailed preparation, incident identification and containment, incident investigation, and remediation and follow-up with lessons learned.

UK Finance recognise the importance of crisis management exercising, and has been organising multi-firm cyber simulations to encourage participation from a range of members in planning for 'when' a cyber attack strikes, rather than 'if'. This complements the partnership between UK Finance and National Cyber Security Centre (NCSC) to set up the Financial Services Cyber Collaboration Centre to further enhance sector readiness to detect, respond and protect itself against cyber attacks.

Key questions to ask:

1. Are your exercises and simulations focused upon the response, recovery and communication?
2. Do your exercises involve the correct people and functions in your business and business partners?
3. Are you adequately 'stressing' scenarios that you are testing as part of your response and recovery preparation activities?

8. COMMUNICATION

The challenge

A key element of achieving resilience is having a strong communication strategy when an organisation suffers a crisis. Clearly and effectively communicating during a crisis can help mitigate some of the disruption experienced by consumers, clients and the broader system. However, the complexity of operating environments, challenges posed by incomplete or potentially inaccurate information and the pace that news can spread pose significant challenges during a disruptive event.

The impact of social media has also meant that firms need to be able to provide consistent public response across a range of platforms in a short space of time. The traditional holding statements provided by firms will no longer be sufficient when an incident occurs.

Firms need to ensure they have a communication strategy that focuses on the following elements: timeliness, clarity and regularity. It should provide information that is actionable and include a clear expectation of when stakeholders will receive further updates.

When revisiting their resilience capability, firms need to determine a clear approach to communication, training and rollout. They will also need to revisit media and communications plans to ensure scenarios and playbooks are linked to critical services.

Perspectives to consider

A range of internal and external stakeholders need to be informed in a timely manner at the beginning of the incident or throughout, as they impact a firm's response to an incident. Information also needs to be passed on externally in a timely manner so that third parties can also advise their clients and stakeholders of any impact on them as a result, helping to address 'ripples' across the system caused by a firm, or firms' own issues.

Firms should consider reviewing and enhancing their crisis communication strategies and response plans to support more timely, regular and insightful communication to stakeholders. One area of focus for some firms is to align messages and stakeholder communications to their most important business services, as traditional playbooks have focused on generic or firm-wide events.

Any crisis communications strategy should be supported by processes and technology solutions to support the effective execution of crisis communications, ensuring that arrangements are tested on a regular basis. Many firms are trying to keep pace with the speed of customer reaction and feedback by proactively monitoring social media for indications that a disruption is occurring.

Many organisations are preparing crisis communications playbooks, including template messaging to improve their speed to communication in a crisis. These templates might require modification during an incident to include key details such as the nature and degree of impact on clients and interested parties. Playbooks might also provide guidance on who or which team needs to approve the updated template communications to make it clear how they should be used.

Firms are reviewing their mechanisms for providing real-time updates to key staff on the status of a service, or on progress of an incident, beyond emails and word of mouth. This is critical to ensure that staff interaction with customers, clients, peers, regulators, the media and other stakeholders are consistent. For many firms branch staff and relationship managers have borne the brunt of customer and client frustration and are relied upon as the 'first line of communication', helping customers and clients directly and promoting the brand through adversity.

Organisations should consider the 'levels', methods and frequency of communication with customers and clients so that they understand the implications of the incident and set expectations ahead of time.

Key questions to ask:

1. How prepared are you to communicate with key stakeholders during an incident in a manner that is timely, regular and actionable?
2. Do you understand how your key stakeholders consume information and what they need from you during a crisis?

Practical next steps

Enhancing operational resilience is likely to be a multi-year effort for all firms. Given the breadth of the topic and the variety of functions and capabilities involved in delivering enhancements, some firms are concerned by the perceived scale of the challenge.

We believe that there are ten basic steps that firms can take to enhance their resilience in the short term, and set the foundations for a more efficient, resilient future state:

1. Identify the most important business services:

a. Agree a list of the most important deliverables or services provided to an end user
b. Link these to business and organisational strategy
c. Use existing views of criticality such as critical economic functions
d. Consider the importance to consumers, markets and the viability of the firm

2. Set impact tolerances:

a. Set a top-down view of the tolerable amount of disruption in all but the most extreme circumstances
b. Test performance against impact tolerances using stress scenarios
c. Review and revisit tolerances upon material change or periodically

3. Understand dependencies:

a. Map business services to supporting systems, third parties, people, facilities, processes and data
b. Be aware of concentration risk and interconnectedness of the ecosystem
c. Identify risks such as single points of failure
d. Understand how the failure of a component could impact the delivery of a business service

4. Assess your current state and test your performance:

a. Understand whether your services and supporting components are resilient enough
b. Develop scenario-driven end-to-end testing
c. Link testing types (scenario, cyber and financial stress) into a portfolio approach and consider lessons learned holistically
d. Establish remediation plans

5. Clearly define ownership:

a. Set out roles, responsibilities and accountability
b. Agree appropriate business ownership of the resilience of important business services
c. Set out tone from the top and define organisational culture
d. Align with the Senior Managers Regime

6. Understand the changing threats you face:
a. Continuously review and update your overall risk profile b. Perform internal and external threat analysis against those risks c. Perform regular horizon scanning to identify potential new risks d. Learn lessons from the incidents that others experience
7. Monitor and report on resilience metrics:
a. Define key risk indicators, and monitor and report against them b. Consider internal and external metrics c. Identify sources of data to provide real-time insights and early warnings d. Develop a strategy to embed continuous monitoring into your future state
8. Embed resilience into transformation and change:
a. Create resilience by design controls based on impact tolerances, ensuring controls and tests are flexed depending on size and scale of change b. Create robust stress testing requirements and define at what stage of change these tests are run prior to going live c. Ensure relevant resilience stakeholders are brought to the table to sign off on controls and design principles d. Embed controls into the change management process, including large-scale transformation
9. Invest in skills and resilient behaviours:
a. Assess the maturity of skills and have an awareness of gaps that need to be addressed b. Develop resilience awareness training across staff groups appropriate to their roles c. Reward resilient behaviours d. Regularly test adherence to resilient practices
10. Define and test communication plans:
a. Identify key stakeholder groups b. Develop communication plans for reasonable scenarios, including during 'black swan' events c. Test communication plans robustly d. Include proactive interaction with regulators

CONTRIBUTORS

ANDREW ROGAN

Director, Capital Markets & Wholesale, UK Finance

Andrew Rogan is head of the Capital Markets teams at UK Finance. Working with members, government and other key stakeholders, Andrew's focus is on delivering outcomes with respect to the operation of global wholesale capital markets, operational resilience, client assets, custody services, and financial markets infrastructures. Prior to joining UK Finance, Andrew served in various roles in central government in both the UK and in Australia.

NICHOLAS EDGE

Principal, Prudential and Foreign Banks Policy, UK Finance

Nicholas works on regulatory initiatives as they impact prudential risk, capital and liquidity management at UK Finance. Nicholas joined UK Finance from an investment bank working in regulatory management. Prior to that Nicholas worked for the PRA (originally FSA) as a Supervisor and also at the Bank of England in Financial Stability, Strategy and Risk.

ALI KAZMI

Partner, Financial Services Advisory, Ernst and Young LLP

Ali is a Partner with more than 18 years of experience supporting clients in managing technology, third party, operational and cyber risk and resilience. He is seasoned in supporting clients with enhancing the resilience of their technology and operational environment, and has led multiple high-profile post incident reviews in the sector in recent years. He also works closely with clients to help them to understand, translate and comply with regulatory requirements and expectations for operational resilience.

CHRIS RICHARDSON

Partner, Financial Services Advisory,
Ernst and Young LLP

Chris is a Partner at EY with more than 20 years of experience supporting clients in managing operational risk across the first and second lines of defence. He is seasoned in supporting clients with operational risk framework design, implementation, embedding and alignment of risk frameworks with operational resilience techniques and approaches. He also works with clients on change management and has led s.166 reviews of change and operational risk at global organisations.

JASON MCLEAN

Partner, Financial Services Advisory,
Ernst and Young LLP

Jason is a Partner at EY with more than 20 years of experience advising boards and executives teams on business strategy, digital programs and organisational restructures to deliver growth targets, efficiencies and enhance resilience. He is seasoned in supporting clients to develop and deliver strategies that leverage modern technologies and build resilience into their global transformation programs.

STEVE HOLT

Partner, Financial Services Advisory,
Ernst and Young LLP

Steve is a Partner at EY with more than 25 years of experience advising senior executives and multi-national organisations on technology risk and cyber security. He is seasoned in supporting clients to enhance their cyber resilience through a range of solutions including, cyber strategy and target operating model transformation, penetration testing, privacy risk management, identity and access management and cyber simulations and stress testing.

MARIA BOND

Senior Manager, Financial Services Advisory, Ernst and Young LLP

Maria is a seasoned management consultant whose primary focus over the last decade has been on articulating the case for large-scale transformational change and taking clients from thought to finish – by helping them to deliver upon their transformation objectives. Her domain experience lies in the strategy, operating model design, digital transformation programme delivery and resilience space. Her consulting experience spans both mature and emerging markets including the UK, Australia, Asia Pacific and the United States, giving her a global perspective on multiple markets, technology trends and industry practices.

EMMA MCKECHNIE

Manager, Financial Services Advisory, Ernst and Young LLP

Emma works within the cyber team at EY supporting clients to better manage cyber, technology and privacy risks as part of an integrated approach to achieving operational resilience. She has a range of major transformation and compliance program experience, including working with a global financial institution to clearly demarcate roles and responsibilities for resilience following integration and demerger activities.

WILL ELLIS

Manager, Financial Services Advisory, Ernst and Young LLP

Will works within the operational resilience team at EY supporting clients in managing technology risk and enhancing operational resilience. He has a broad range of experience supporting clients from large global financial institutions through to small FinTechs with their approach to operational resilience. This includes leading operational resilience capability assessments, advising on regulatory engagement, performing high-profile post-incident reviews and facilitating incident and crisis simulation testing. Will is also focused on the intersect between operational resilience and other existing and emerging regulatory requirements including PSD2.