www.pwc.co.uk

Becoming operationally resilient

A guide to operational resilience in Financial Services

4 July 2018

Contents

Executive summary

Operational Resilience is a subject that has risen to increased prominence over recent years and this trajectory is unlikely to change in the foreseeable future. Technology advances allied to increased consumer demands create an increasingly challenging environment in which to deliver services. Meanwhile, instant and high-profile feedback through social media elevates resilience issues to a new level of scrutiny. Recent prominent and sustained incidents have made operational resilience topical, while regulators continue to enhance their expectations on resilience capabilities.

Regulators are requiring firms to make substantive developments to their approaches to resilience, while the crystallisation of a resilience issue heightens supervisory focus on a firm. In this environment, regulatory pressures are undoubtedly a strong driver for firms to evolve their approaches to resilience.

There are, however, wide-reaching benefits to be achieved in delivering effective operational resilience that go far beyond mitigating risk of regulatory sanction and limiting downside risk.

Organisations can achieve a quicker and more measured management of incidents by accepting that resilience events are inevitable. Accepting that encountering resilience events is a question of ‘when’ rather than ‘if’, can help to move a firm beyond the first three stages of reaction to an unexpected event (typically surprise, anger, resistance) towards acceptance, where the issue can be managed far more effectively.

Other benefits of improved approaches to resilience are the ability to make better decisions at a senior level based on an understanding of the robustness of the organisation; closer alignment between the business and the sources of operational risk; and ultimately an ability to increase customer trust and reduce the risk of reputational damage.

Making the required change to achieve effective management of operational risk often necessitates a step-change in mindset. Resilience has often been considered a business continuity and disaster recovery issue, but in reality it is much wider reaching. It also requires a broader set of skills and specific ownership. With the advent of the Senior Management Function (SMF) 24 role, the responsibility for operational resilience may have a somewhat more intuitive home, while the skills required to fulfill an operational resilience capability may need to be drawn together either formally or as a virtual team.

Creating clarity over your organisation’s definition of resilience and the mandate of the operational resilience capabilities, enables you to set the standard by which your organisation should operate. You should follow this up with an assessment of your organisation’s current operational resilience maturity along with a view of your ambition regarding the capability. Doing this provides you with the basis from which you can deliver transformation in your organisation, but your aim should be to get to the point of ‘business as usual’ and sustainable management of operational resilience. You can achieve this by creating a clear and repeatable analysis of product and service criticality, and mapping relevant processes end-to-end. Once this is achieved, including a view of the underlying involvement of the four pillars, or resource enablers, of technology, people, premises and suppliers, it is possible to identify key points of failure and key points of control. These are the areas to focus on in creating resilience.

Regulatory and consumer expectations are likely to continue to rise, putting pressure on firms to develop more sophisticated approaches to resilience. Developments in artificial intelligence and data analytics, combined with a strong culture and a fearless attitude toward dealing with issues head-on will lead to more influential and effective resilience capabilities. Importantly, this will also create an opportunity for markets to differentiate between organisations based on their stability and resilience.

Reader guide

This document aims to provide insights to a wide range of readers, and we are aware that some sections are more relevant to some readers than others. Therefore, the structure of the document is outlined below, along with an indication of how relevant each chapter is to each reader group.

	1. Executive summary	*2. What is operational resilience?*	*3. Why focus on operational resilience?*	*4. Delivery operational resilience*	*5. Extensions of operational resilience*	*6. Future of operational resilience*	*7. Regulatory environment summary*
CEO	① 2 3	1 ② 3	1 ② 3	1 2 ③	1 2 ③	1 2 ③	1 2 ③
CIO/COO	① 2 3	① 2 3	① 2 3	① 2 3	① 2 3	1 ② 3	1 ② 3
CRO/CCO	① 2 3	1 ② 3	1 ② 3	1 2 ③	1 2 ③	1 2 ③	1 2 ③
Head of resilience	① 2 3	① 2 3	① 2 3	① 2 3	① 2 3	1 ② 3	1 ② 3
CTO	① 2 3	1 ② 3	1 ② 3	① 2 3	① 2 3	① 2 3	1 2 ③
Business leader	① 2 3	1 ② 3	1 ② 3	1 2 ③	1 2 ③	1 2 ③	1 2 ③
Operational risk	① 2 3	① 2 3	① 2 3	① 2 3	① 2 3	1 ② 3	1 ② 3
Compliance	① 2 3	① 2 3	1 ② 3	1 ② 3	① 2 3	1 ② 3	① 2 3
Internal audit	① 2 3	1 ② 3	1 ② 3	1 ② 3	1 ② 3	1 ② 3	1 ② 3

① 2 3 Essential reading 1 ② 3 Important reading 1 2 ③ Discretionary reading

Introduction

Backdrop

Our interest in Operational Resilience is not new. Since 2011, we have remained as central to the development of this discipline as possible. Our involvement in the investigation and remediation of a bank's major technology and service outage in 2012 was a tipping point not only for us, but for the industry and regulators as a whole. The transformation that has been sustained by many of our clients has been significant and impressive. Now, six years later we see an increasing focus and the prospect of much greater regulatory scrutiny across the breadth of the financial services industry.

We see the next chapter for the industry as the development of sustainable competitive advantage through being operationally resilient. Of course, this will also have industry-wide benefits in terms of security and safety. We want to contribute to a shift in the debate to a more positive rhetoric and value adding benefits. We want our clients and the industry to prosper as a result of good operational resilience outcomes. We are sharing the results of six years of working with dozens of firms from the very largest multinationals to smaller firms across the spectrum of financial services. We share insight from insurers and asset managers as well as retail and investment banking and financial market infrastructure firms. We have also had the opportunity to work directly with regulatory organisations as they have developed their thinking in this space.

Roads to ruin

Increasing reliance on technology and heightened regulatory attention mean that operational resilience is a hot topic across the industry, but the need to be resilient is not new. In 2011 alongside the Cranfield School of Management and Airmic, we published a report on the origins and impact of over twenty major corporate crises. We traced the deeper causes of these crises, to assess the post-event resilience of the firms involved and considered the implications for risk management more broadly. The crises we examined involved substantial, well-known organisations across a range of industries including Airbus, Société Générale, Northern Rock, AIG, Independent Insurance, Enron, Arthur Andersen as well as smaller firms.

We provided over 100 lessons about risk, risk analysis and risk management in the context of critical events. Several of the firms we studied were destroyed by the crises that struck them. Others survived, but they often did so with damaged reputations and facing the uphill task of rebuilding their businesses. Significantly, we found that the firms most badly affected had underlying weaknesses that made them especially prone both to crises and to the escalation of a crisis into a disaster.

Substantial improvements have been made by financial services firms in recent years, but high-profile incidents at major banks show that many of the weaknesses we identified, such as board risk blindness, defective communications and excessive complexity are still common. The current environment means that stakes have never been higher and financial services firms, senior leaders and risk professionals need to ensure that operational resilience is managed with enhanced vision and competencies to protect the profitability and reputation of their organisations.

Roads to resilience

Building on 'Roads to Ruin' and again alongside Cranfield and Airmic, we produced 'Roads to Resilience' in 2013. We conducted primary case studies and analysed the ways in which risk is managed in order to achieve greater resilience. We focused on eight firms across different sectors and found that these organisations go far beyond what would normally be considered risk management.

In the eight organisations studied, the traditional tools, techniques and structures of risk management were understood and extensively applied. However, it was clear that these approaches, whilst regarded as necessary by management, failed to achieve the desired level of organisational resilience. The best organisations were found to be adaptive to change, as they do not just focus on building stronger defence mechanisms. Instead, they build the capability to deal with both the expected and unexpected, protecting reputation and integrity, while still remaining focused on their business goals.

We sought to highlight the business drivers for rigorous operational risk management and identified that resilient organisations not only develop the ability to quickly identify emerging risks, but they are also better placed to recognise and take advantage of the upside of risk-taking – opportunity.

Roads to reward

Now, in 2018, we are providing a series of perspectives to help firms develop their operational resilience. We have interviewed a number of clients and aggregated our views on both emergent and best practice across financial services. Our focus has been to identify the broader rewards and benefits that can be achieved through the development of an effective operational resilience capability.

I do hope you find this report informative and valuable and I look forward to the conversations on this topic in the months and years to come.

Simon C Chard
Financial Services Partner, PwC

1. What is operational resilience?

“Incidents are inevitable, how firms recover is what differentiates them.”

– *Head of Resilience at a leading UK retail bank*

Chapter summary:

The definition of operational resilience has evolved since the Bank of England coined the term in 2015. Operational resilience can be defined as ‘an organisation’s ability to protect and sustain its core business functions when experiencing operational stress or disruption’. The scope of operational resilience goes beyond that of traditional Disaster Recovery and Business Continuity Planning and views services from a customer point of view in order to protect the processes that are the most critical.

Defining operational resilience

Definitions of operational resilience have evolved since the Bank of England (BoE) offered an interpretation in its 2015 Dear Chairman Letter II glossary as ‘an organisation's ability to protect or sustain its critical functions, and underlying assets, while adapting to expected or unexpected occurrences of operational stress or disruption’. Since then, the sector has debated the scope of this definition, in terms of both defining the critical services and how to differentiate between what to protect and what to sustain.

Charlotte Gerken, Director, Supervisory Risk Specialists at the BoE, defined operational resilience in a June 2017 speech at the Operational Risk Europe 2017 Conference as: ‘the ability to adapt operations to continue functioning, when – not if – circumstances change’. Clearly, it is likely that the definition of operational resilience will continue to evolve, but Gerken’s interpretation is useful because it underlines the importance of accepting the inevitability of resilience events. Indeed, a key challenge for firms is to accept that it is not possible either to predict or prevent every possible event. Many organisations have been on a journey of understanding and accepting this reality, often involving challenging conversations at Board-level along the way. Financial services firms which achieve this acceptance, and can translate it into a defined resilience risk appetite and risk tolerances, are better placed to respond quickly, decisively and effectively when adverse situations arise. Lyndon Nelson, Deputy CEO, Executive Director at the BoE speaking at the 2018 Operational Risk Europe conference suggests this means that firms will ‘be on a WAR footing: withstand; absorb; recover.’ Both speeches provide a clear outcome that organisations should seek to achieve, namely the continuation of service during disruption. This perhaps differs from the objectives of previous continuity programmes which purely focused on the preservation of the firm and the interests of its shareholders, notwithstanding their ability to provide an appropriate level of service to customers.

Looking beyond the BoE’s definition, the evolution of new risks, emerging technology and an increasingly connected industry has resulted in a clear increased regulatory focus on resilience and an evolving picture of what resilience means. Of late, regulators have placed particular focus on potential detrimental impacts on consumers. As regulators articulate their understanding and expectations, they are becoming increasingly prescriptive in their requirements. We explore current and potential future regulatory supervisory trends in chapters 5 & 6.

In previous cases of newly established disciplines or regulatory areas of focus, the rush to frameworks and methodologies is commonplace. Examples in recent times include ‘Treating Customers Fairly’ or conduct risk management. In contrast to this approach, we see operational resilience as an outcome that firms should seek to achieve, rather than a defined process or methodology. Being resilient is a continuous way of working that should become part of your everyday offering to your customers. The target should be to become resilient, not to seek the impossible goal of eliminating the myriad risks your organisation encounters.

Organisational scope of operational resilience

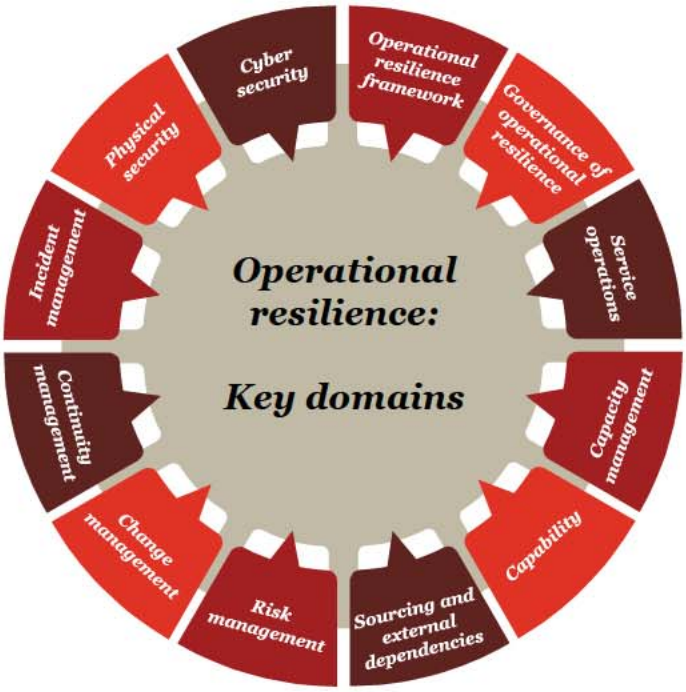
Accepting that to achieve the outcome of resilient critical services you must look broader than Business Continuity and Disaster Recovery, enables those responsible for achieving it to explain to the business more clearly the change in scope. Too often we have seen Business Continuity or Disaster Recovery teams simply rebranded as 'operational resilience' without changing the scope or outcomes they are seeking to achieve. In these cases, such new functions are often met with scepticism and resistance within the broader organisation.

So, if operational resilience is not simply the rebranding of Business Continuity and Disaster Recovery, what is it? If we start from the basis that we want to protect those services provided to customers and clients that are deemed critical, we need to consider the processes that underpin the delivery of these services both internally and externally. While Business Continuity and Disaster Recovery are part of the answer, they are not the complete picture. The scope of operational resilience is very broad and encompasses many different areas within an organisation, often necessitating the breaking down of existing silos in the process. This may not call for the development of an all encompassing operational resilience team or business unit, but it does require consensus of what is critical and an agreed common purpose to deliver a resilient service to customers and clients.

Beyond existing definitions

During the past year, the Prudential Regulation Authority (PRA) has been increasingly interested in operational resilience beyond what might be considered the traditional IT-related areas. Where organisations have been required to take action, the use of the 'customer lens' in reviewing operational resilience has resulted in focus on areas such as client onboarding, sanctions screening and other regulatory or compliance related processes. These are prime examples of areas where failures could impact a wide spectrum of customers and firms could experience significant reputational risk as a result.

Similarly, the storage and maintenance of customer data is increasingly considered from an operational resilience perspective by firms and regulators. Given the impact of failures in this area on customers and the new GDPR environment, establishing strict protocols and controls is paramount. In the event of a breach or issue, swift resolution is likely to be critical to minimising operational and reputational impacts.



Forming a view of the factors above in the context of the organisation is a critical first step. Once a definition and desired outcome have been determined by your organisation, it then becomes possible to embark on the process of delivering operational resilience.

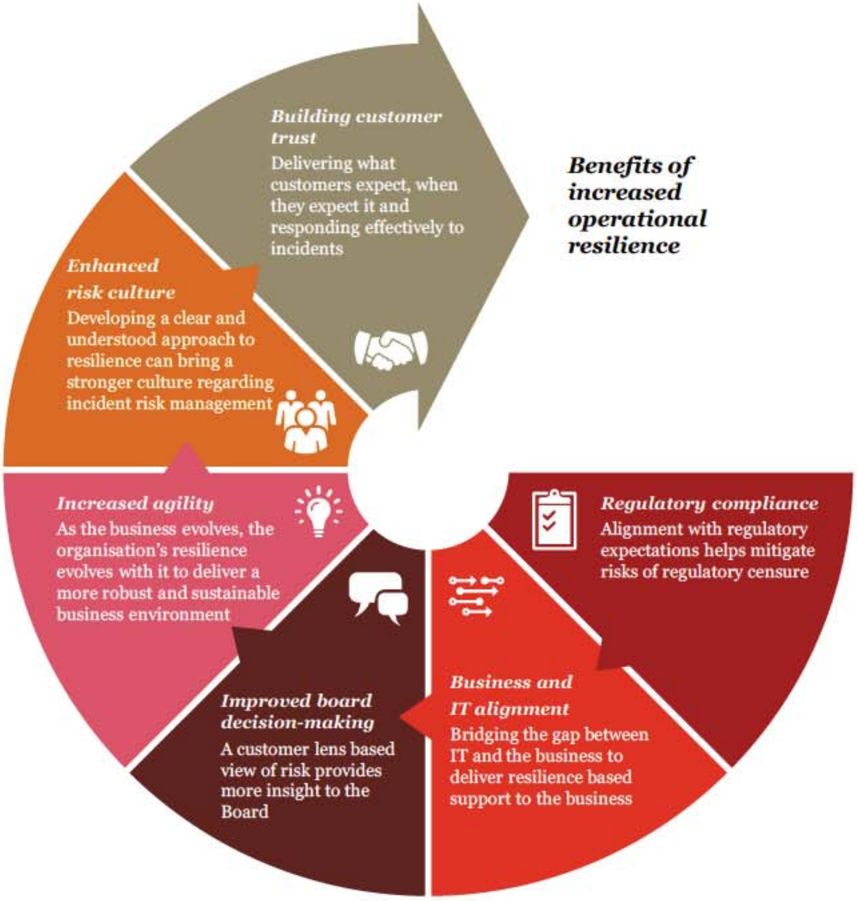
2. Why focus on operational resilience?

> *"A forward-looking, proactive operational resilience function facilitates an agile culture as it enables tech teams to design systems and processes with resilience in mind."*
>
> – *Head of Resilience and Continuity, multi-sector bank*

Chapter summary:

To date many financial services firms have viewed operational resilience through a regulatory lens leading some to think of it as 'just another thing to comply with'. However, having a highly resilient, adaptable and risk aware organisation allows firms to capitalise on a range of business benefits. Meeting regulatory expectations is the bare minimum level of maturity that firms should be aiming for. Developing a robust, forward looking operational resilience capability allows firms to evolve their services with confidence, make better board and investment decisions and build customer trust.

As we have already outlined, there is an established regulatory imperative in place for firms to address, but the benefits of delivering an increasingly resilient and robust organisation are more significant than this. Developing a robust view and approach to operational resilience initially may result in incurring cost, but establishing an organisation that is predisposed to respond to adverse situations quickly, effectively and decisively can deliver cost and reputational benefits down the line. In this section, we outline the benefits of sound operational resilience based on our experience of working with financial services organisations.



Benefits of increased operational resilience

Regulatory compliance
Alignment with regulatory expectations helps mitigate risks of regulatory censure

Business and IT alignment
Bridging the gap between IT and the business to deliver resilience based support to the business

Improved board decision-making
A customer lens based view of risk provides more insight to the Board

Increased agility
As the business evolves, the organisation's resilience evolves with it to deliver a more robust and sustainable business environment

Enhanced risk culture
Developing a clear and understood approach to resilience can bring a stronger culture regarding incident risk management

Building customer trust
Delivering what customers expect, when they expect it and responding effectively to incidents

Regulatory compliance

As previously noted, regulators are increasingly focused on operational resilience, drawn by the risk to consumers as well as the financial stability risks operational outages can bring. Increased regulatory intervention has helped to raise the profile of effective operational resilience, but in reality, being compliant and mitigating risk of regulatory censure should be the minimum expectation for an operational resilience capability.

The PRA's discussion paper will provide the clearest steer to date on regulatory thinking and provide minimum standards for firms to achieve, but a well designed and effectively implemented operational resilience programme should have few problems meeting regulatory expectations and should in fact deliver the wider benefits explored below.

Better IT and business alignment

A robust and capable operational resilience capability can help bridge the gap between the business and IT by translating business priorities into technology controls. Highlighting the importance of technology in underpinning key business processes and engaging the business when making decisions over desired resilience levels encourages a joined-up approach. Eliminating gaps and overlaps through a seamless approach to resilience, combined with a greater focus on the areas that really matter, will make operations more efficient and resilient. If operational resilience approaches are customer focused, it can enable them to engage with senior business and technology leaders to underline the importance of resilience to both business and technology teams.

Improved board decision making

Understanding the end to end delivery of a critical customer or client service (including process, technology, data, third parties, people and premises) allows organisations to look at risks and mitigating controls comprehensively. This facilitates understanding of the moving parts in a context aligned to the customer's view. While component parts of this view are held within organisations, it is rarely viewed in this holistic context.

Too often, risk information provided to boards is too detailed and based on risk taxonomies (e.g. cyber risk, financial crime risk), rather than on a more intuitive view of the customer service process. A customer-centric view of operational risk and resilience allows board-level leaders to make better investment and risk decisions based on potential impact to customers.

As firms seek to adapt and evolve more rapidly, it is likely that they will consider buying in services and solutions, including offerings from FinTech providers specialising in specific areas. While the benefits of this approach are numerous, it brings further risk into the business and presents another potential source of interruption in services to customers and clients. By understanding the criticality of services from inception, it is possible to ensure services are aligned with your organisation's overall resilience profile and allow you to establish appropriate control and ownership.

Increased agility

The financial services industry is changing faster than ever. To stay competitive firms must move quickly to take advantage of new opportunities. A past criticism of operational resilience and other risk management functions is that they slow down innovation to control risk. To compete with new FinTech firms and to take advantage of market opportunities, large financial services firms are being forced to become increasingly agile. Effective operational resilience capabilities give firms the ability to adapt their current approach to facilitate rapid change in a controlled manner.

Delivering operational resilience support from project inception and through each subsequent stage can help assure the design, develop controls and embed resilience methodology throughout. Achieving this requires close alignment between operational resilience and company sandboxes and innovation centres to identify and prepare for new technologies in a more proactive way. This approach will help to identify, prioritise and mitigate risk from an early stage.

An enhanced risk and response culture

The process of identifying potential risks to your organisation's resilience, along with the achievement of a higher profile for the discipline will help drive a change in your organisation's risk culture. In the case of resilience, speed of response to issues is paramount. Time spent in panic mode, trying to work out what to do and who is doing it all contribute to ineffective responses.

Effective protocols for response, clarity of owners and a measured approach lead to an organisation that understands the concept of resilience and can manage issues well. The need to achieve this clarity is underlined by the Senior Managers Regime (SMR) and specifically the SMF24 (Chief Operations Officer) role, which specifically identifies responsibility for resilience capabilities.

Elevating the profile of operational resilience helps create a shared language in relation to the subject and a better understanding of the role it plays in your organisation. It's likely there will always be individuals who revert to a 'panic stations' mentality under stress, but engineering a capability and culture in relation to resilience will go a long way to help your organisation to think and behave appropriately under pressure. Ultimately, it is important that risk and response actions and activity improve, or at least contain an incident, rather than make the situation worse. *'Behaving well in a bad situation is better than behaving badly in a good one' Head of Resilience and Continuity, multi-sector bank.*

Customer trust

'Operational Resilience is the core of the promise that firms make to their customers' Christopher Woolard - PwC webcast – 15 May 2018.

In a world that is increasingly reliant on technology, and often demanding a shift to the latest technology, customers and clients have expectations that services are available at any time. To meet this demand, organisations must adapt at far greater speeds than ever before. Subsequently, understanding what is critical in customer services and what supports them is essential.

Delivering a service that is robust and responsive in the event of issues occuring is the minimum expected by customers and clients. Recent incidents in the industry have resulted in sustained outages and impacted customer trust. An effective operational resilience capability is essential to rebuild or cement the trust between organisations and customers.

Firms across the sector are embracing the digital agenda but this brings risk into ways of working that could have dramatic consequences if things go wrong. Over the past six years, we have seen numerous technology outages or incidents across the sector that have happened as a result of poor technology management. Understanding what is critical, including the underlying technology and data, will allow for better change management and incident response when things go wrong.

Protection of reputation and customer trust is paramount to any incident response but failure in communications to customers and media handling is a common issue. The rise of social media and heightened media coverage in general have shone a light on incidents in a way not previously experienced. This increased scrutiny means even small outages can be damaging and underlines the need to proactively minimise the likelihood of incidents and formulate better responses and communications when things go wrong. Doing so will help build customer trust and allows your organisation to differentiate itself in the market.

3. Delivering operational resilience

> *“We have an approach based on critical business process which shines a light on areas that require it and gives the Board the information they need to make risk based decisions.”*
>
> – *Director of Group IT, Security and People Risk at major UK retail bank*

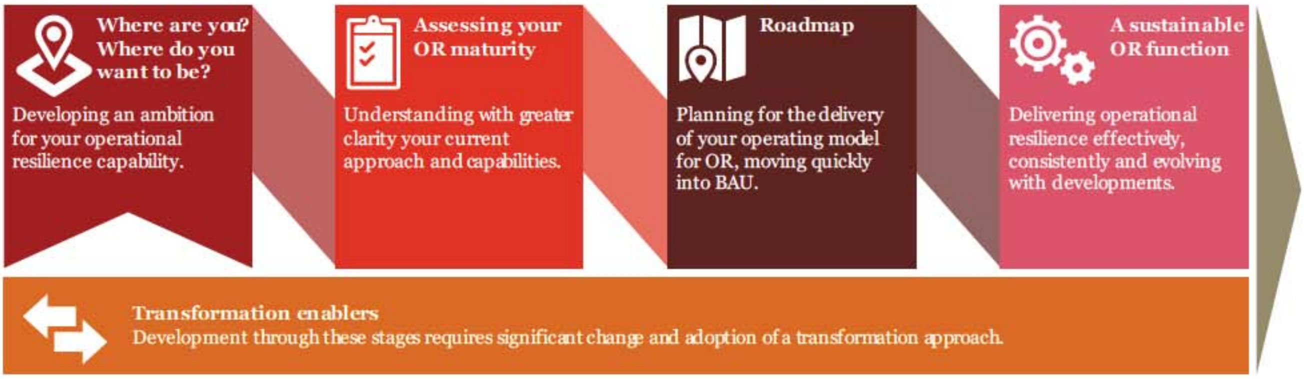
Chapter summary:

Many financial services firms already have component parts of an operational resilience framework in place. To develop these current practices firms should take the time to evaluate their current and desired maturity levels and build a roadmap to achieve the desired state. In this section we detail PwC’s bespoke approach to developing an operational resilience function that meets regulatory expectations and delivers measurable business benefit in the financial services sector. Whilst many firms use a programme/project delivery mechanism to achieve change in the short term, firms should be prepared to transition to a sustainable business as usual approach as the capability matures.

Across the financial services industry we have observed organisations that already have many of the component parts of a resilience framework in place. Your firm can use these elements as a foundation from which to grow your resilience capability. Value comes from bringing these parts together, operating within a common resilience framework and integrating risk indicators into the programme in a coordinated manner.

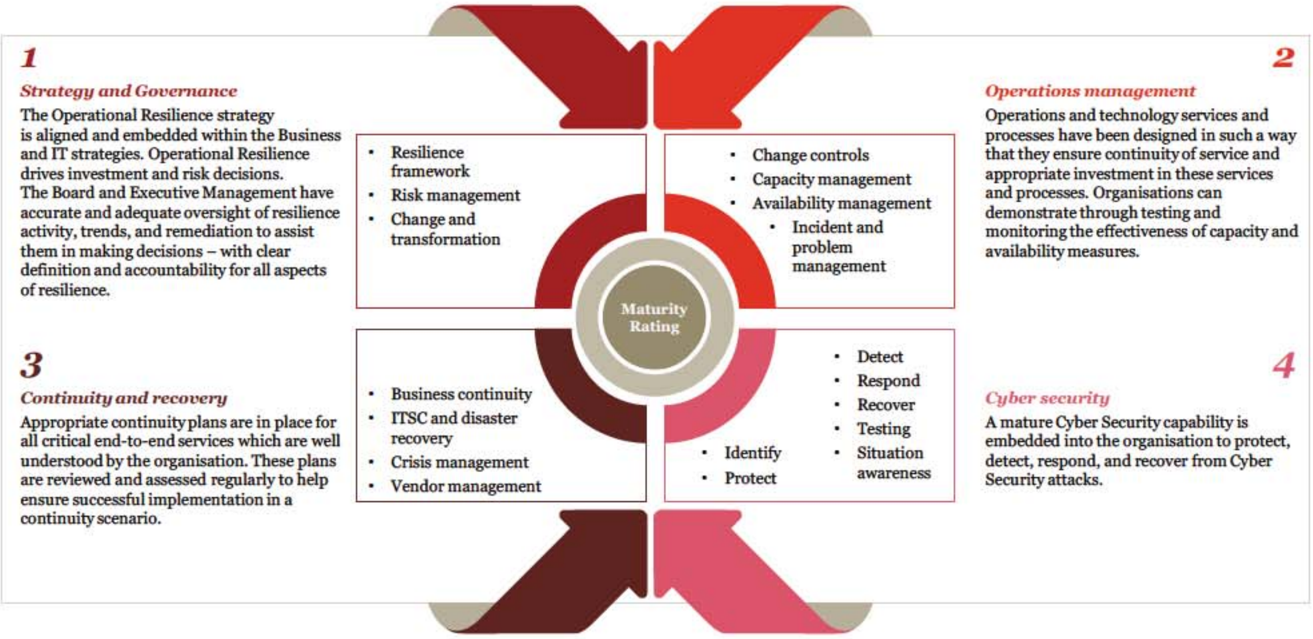
Commonly, there are varied levels of capability across the four pillars (or resource enablers) we consider in operational resilience (technology, people, premises and suppliers). While management and ownership of these disciplines should remain with the appropriate leaders within business units, the reporting of the risks and capabilities must be consolidated and related to end to end business processes and critical services. This should be underpinned and supported by a common approach and rigorous governance structure, which aligns to leading practice in financial services organisations.

Identifying where to begin can be a daunting process, as can deciding to embark upon refreshing your view of your organisation’s capabilities. Within this section, we outline some of the processes or methodologies that can help move you forward quickly in the early stages and translate into strategic development in the medium to long term.


Where are you? Where do you want to be?
Developing an ambition for your operational resilience capability.
Assessing your OR maturity
Understanding with greater clarity your current approach and capabilities.
Roadmap
Planning for the delivery of your operating model for OR, moving quickly into BAU.
A sustainable OR function
Delivering operational resilience effectively, consistently and evolving with developments.
Transformation enablers
Development through these stages requires significant change and adoption of a transformation approach.

Where are you now? Where do you want to be?

Before your organisation embarks on a programme of work it is often helpful to first undertake an exercise to determine your current level of maturity or capability versus your desired state. This provides a high-level indication of the scale of change required and is an important tool for communicating and agreeing the desired state with senior management.



1

Strategy and Governance

The Operational Resilience strategy is aligned and embedded within the Business and IT strategies. Operational Resilience drives investment and risk decisions. The Board and Executive Management have accurate and adequate oversight of resilience activity, trends, and remediation to assist them in making decisions – with clear definition and accountability for all aspects of resilience.

- Resilience framework
- Risk management
- Change and transformation

2

Operations management

Operations and technology services and processes have been designed in such a way that they ensure continuity of service and appropriate investment in these services and processes. Organisations can demonstrate through testing and monitoring the effectiveness of capacity and availability measures.

- Change controls
- Capacity management
- Availability management
  - Incident and problem management

3

Continuity and recovery

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

- Business continuity
- ITSC and disaster recovery
- Crisis management
- Vendor management

4

Cyber security

A mature Cyber Security capability is embedded into the organisation to protect, detect, respond, and recover from Cyber Security attacks.

- Identify
- Protect
- Detect
- Respond
- Recover
- Testing
- Situation awareness

Once your organisation has made the decision to develop an approach to operational resilience it can often be unclear where to begin due the many disciplines involved. In most cases, the sensible approach is to build from an established business continuity or service continuity team. These teams are often best placed as they already interact across the four resilience pillars and provide much of the data and MI required for resilience.

In terms of ownership and responsibility, under the SMR framework, the SMF 24 holder would be a natural leader for this kind of project. The definition of SMF 24 in the PRA handbook is 'responsibility for managing the internal operations and technology of a firm'. This role and its relevant requirements came into force in November 2017.

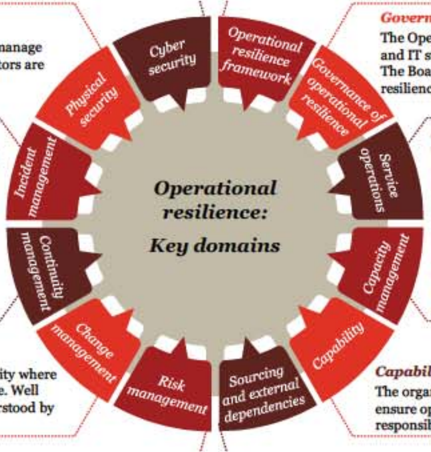
The PRA expects that the SMF 24 responsibilities may include, but not necessarily be limited to, areas such as:

- Business continuity;
- Cybersecurity;
- Information technology;
- Internal operations;
- Operational continuity,
- Resilience and strategy;
- Outsourcing, procurement and vendor management; and
- Shared services.

Assessment of maturity

By assessing your organisation's current arrangements and identifying your operational resilience ambitions, you can prioritise your change programme. This will allow you to deliver in the areas which require the most attention. Once implemented and embedded, your resilience programme will be demonstrably sustainable through sound governance and reporting.

There are a number of key areas that define a successful resilience programme. These areas should be reviewed prior to the commencement of any transformation work. Through our experience working with clients we have defined these areas as shown below:



Cyber security

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

Physical security

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

Incident management

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

Continuity management

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

Change management

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

Risk management

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

Operational resilience framework

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

Governance of operational resilience

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

Service operations

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

Capacity management

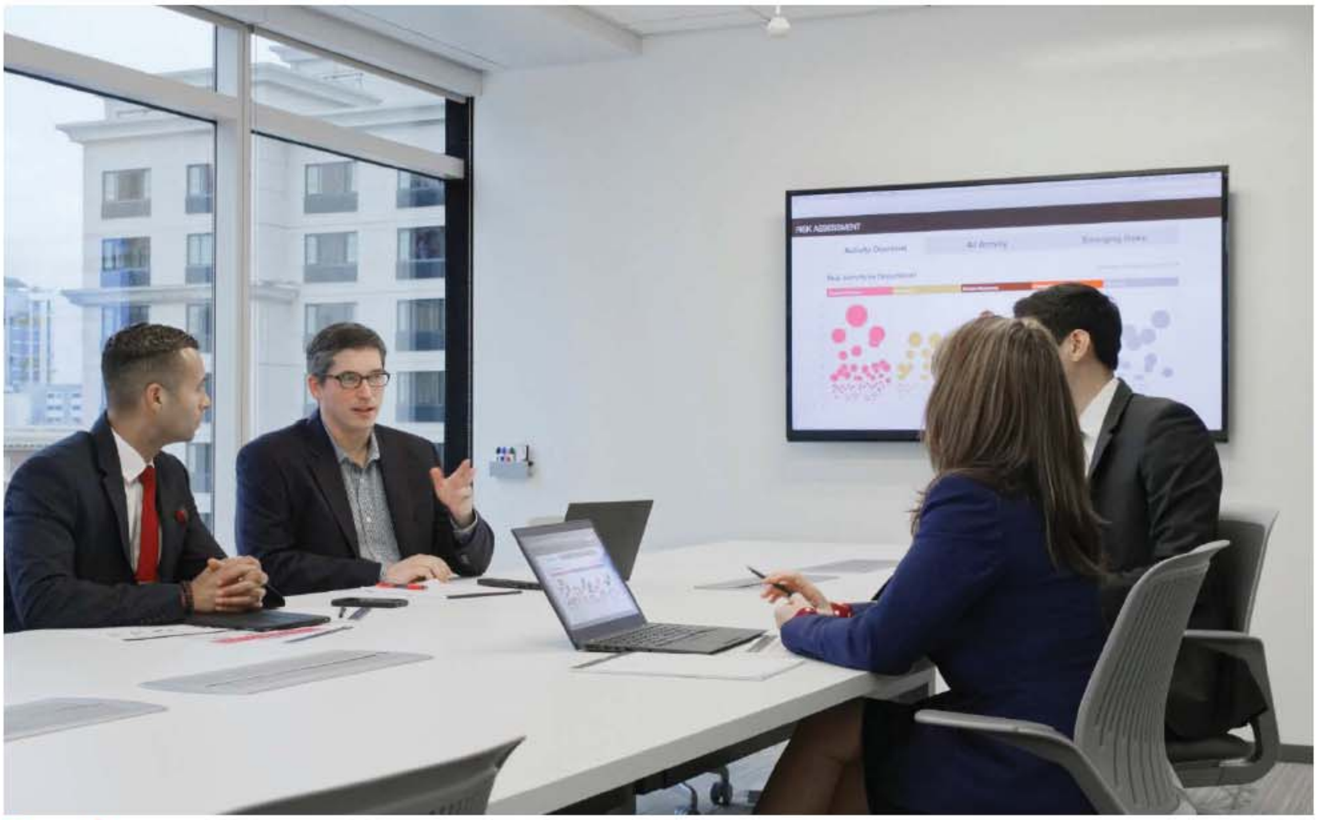
Organisations can demonstrate through testing and monitoring the effectiveness of capacity measures.

Capability

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

Sourcing and external dependencies

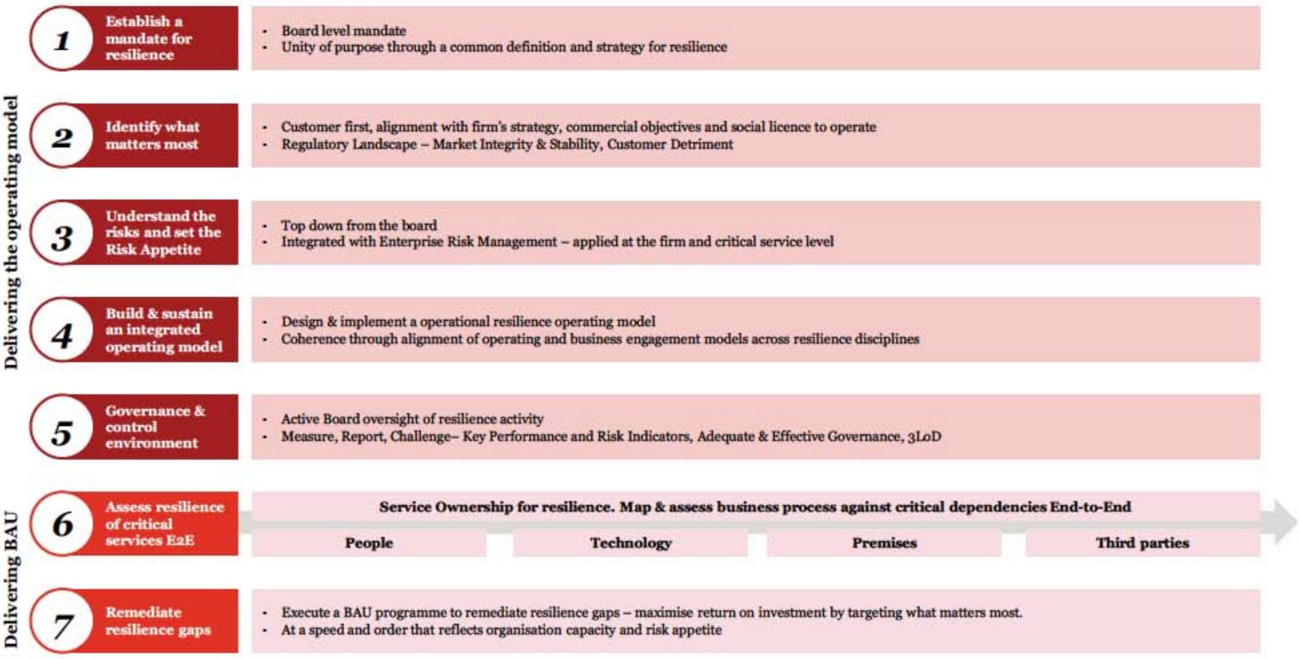
There is clear consideration and understanding of the dependencies on external or sourcing partners and the level of risk that is introduced into the critical services. Performance, risk and effectiveness of these relationships are frequently assessed and understood.



Roadmap

Delivering an operational resilience operating model

After establishing current and desired states, building out a roadmap to facilitate the delivery of the change is a critical outcome. We outline below a high level framework approach to building your resilience capability through focusing on seven areas of activity.



Delivering the operating model

1 Establish a mandate for resilience
- Board level mandate
- Unity of purpose through a common definition and strategy for resilience

2 Identify what matters most
- Customer first, alignment with firm's strategy, commercial objectives and social licence to operate
- Regulatory Landscape – Market Integrity & Stability, Customer Detriment

3 Understand the risks and set the Risk Appetite
- Top down from the board
- Integrated with Enterprise Risk Management – applied at the firm and critical service level

4 Build & sustain an integrated operating model
- Design & implement a operational resilience operating model
- Coherence through alignment of operating and business engagement models across resilience disciplines

5 Governance & control environment
- Active Board oversight of resilience activity
- Measure, Report, Challenge– Key Performance and Risk Indicators, Adequate & Effective Governance, 3LoD

Delivering BAU

6 Assess resilience of critical services E2E

Service Ownership for resilience. Map & assess business process against critical dependencies End-to-End

People | Technology | Premises | Third parties

7 Remediate resilience gaps
- Execute a BAU programme to remediate resilience gaps – maximise return on investment by targeting what matters most.
- At a speed and order that reflects organisation capacity and risk appetite

1. Establish the mandate

This is a fundamental in driving clarity in your organisation over the nature of operational resilience. Having a clear and common definition of what resilience means for your organisation allows you to develop an operational resilience strategy. Executive sponsorship is key to successfully delivering an operational resilience programme, and establishing the mandate and role of a resilience capability. The SMF 24 holder is likely to be a key influencer in this process.

2. Identify what matters most

Identify and agree the critical services and products that your organisation delivers. These should be agreed by the Board and communicated to your organisation. Operational resilience puts the customer at the heart of the criticality assessment. Criticality should align to the business strategy, enable prioritisation of effort and influence strategic decisions.

A good starting point for criticality measurement is the organisation's enterprise risk management framework (ERMF), operational risk management framework (ORMF) or the compliance risk assessment. These generally provide criticality categories, thresholds or parameters which may be suitable for reuse and provide a criticality matrix for assessing risk.

In effective operational resilience the assumption is that failure will occur, so likelihood is not such an important component of criticality measurement. More important is the impact categories, which can be applied with an appropriate assumption for the duration of an outage e.g. service is unavailable for 24 hours. Indicative impact categories include regulatory, legal, customer, people, financial and reputational.

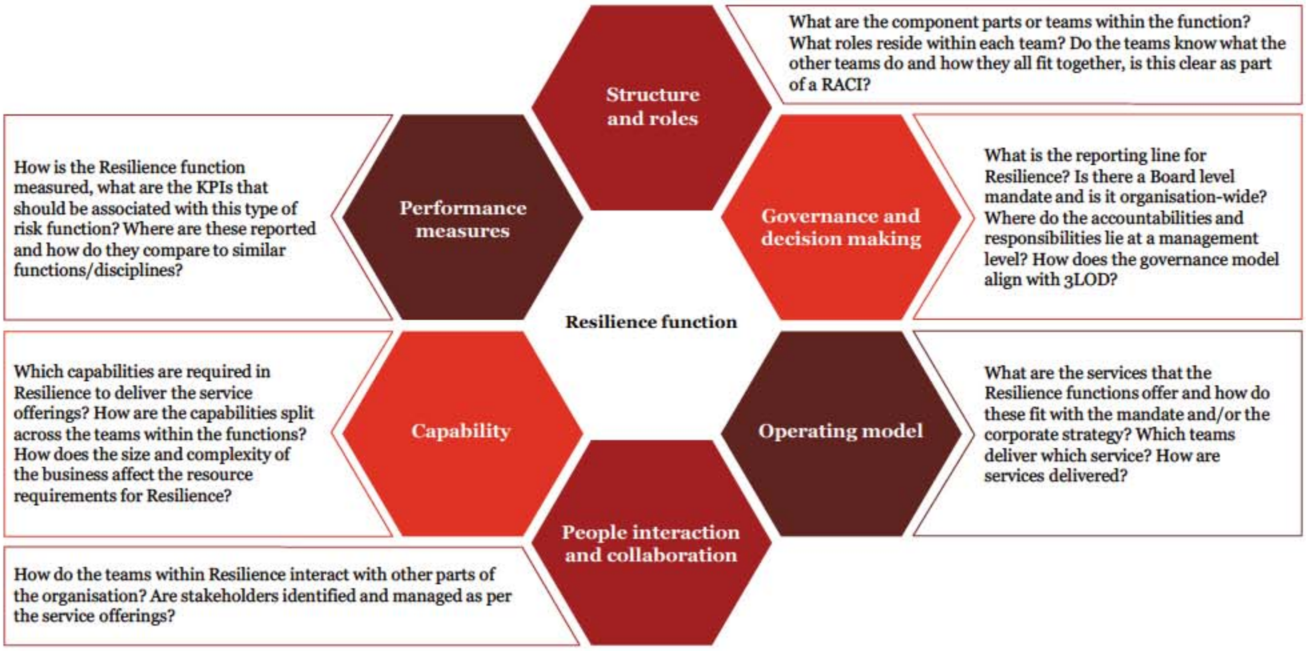
3. Understand the risks and set risk appetite

Once you have established what is critical, the next stage to consider is the level to which you want to achieve protection. Realistically, not every service can be fully resilient, so knowing where your risks and vulnerabilities lie and how you will mitigate them is crucial. Some less critical services will have a period of tolerated outage which must be defined and applied consistently.

There is a regulatory drive to apply a customer-focused lens to your evaluation of criticality. This can be achieved by analysing how likely an outage or key control failure is to impact populations of individuals. Populations can be considered by geography, product type or service used, or financial value of the product to the organisation (a proxy for an impactful product). For example, an outage affecting a smaller location that is characterised as being dependent on your organisation is likely to be considered as an increased risk area from a systemic viewpoint.

4. Build and sustain an integrated operating model

This stage involves designing the actual operating model for delivery of operational resilience. Decisions on where resilience will be owned and if a federated or functionalised model will be implemented are key. There is a potential need to bring together, in a virtual team, the related resilience and security and other disciplines with an appropriate engagement model. Outlined below is our depiction of the key elements of an operating model and some considerations for the design and build of a model.



What are the component parts or teams within the function? What roles reside within each team? Do the teams know what the other teams do and how they all fit together, is this clear as part of a RACI?

How is the Resilience function measured, what are the KPIs that should be associated with this type of risk function? Where are these reported and how do they compare to similar functions/disciplines?

What is the reporting line for Resilience? Is there a Board level mandate and is it organisation-wide? Where do the accountabilities and responsibilities lie at a management level? How does the governance model align with 3LOD?

Which capabilities are required in Resilience to deliver the service offerings? How are the capabilities split across the teams within the functions? How does the size and complexity of the business affect the resource requirements for Resilience?

What are the services that the Resilience functions offer and how do these fit with the mandate and/or the corporate strategy? Which teams deliver which service? How are services delivered?

How do the teams within Resilience interact with other parts of the organisation? Are stakeholders identified and managed as per the service offerings?

5. Governance and control environment

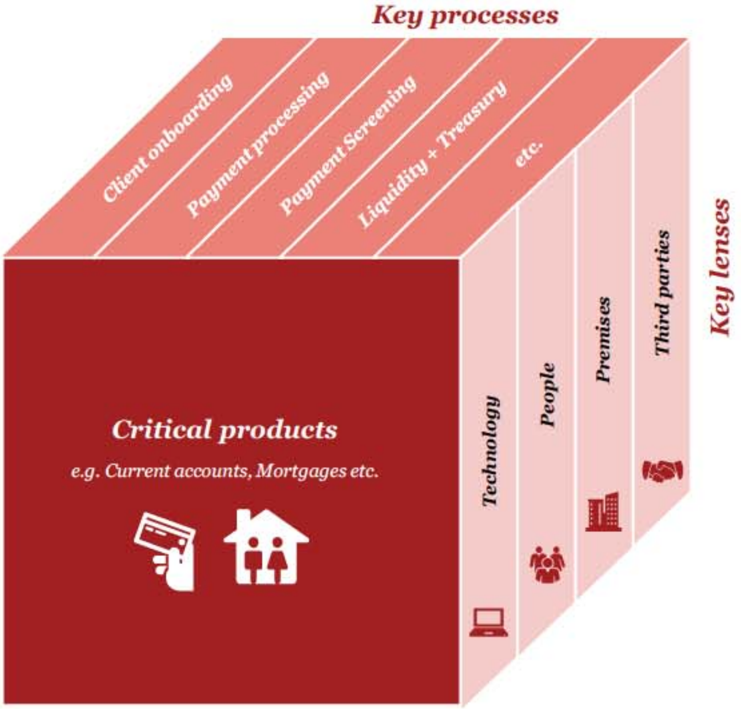
An effective and intuitive governance framework is required to oversee and make decisions over operational resilience considerations. Operational resilience risk can form part of your existing risk governance structure, but terms of reference and reporting may need to be amended to facilitate a new view of resilience. Determining how you will measure and report resilience risk will need to be based on robust and agreed decisions over criticality and areas of disproportionate impact should an issue occur. In terms of a control or policy framework, existing policies in related disciplines will provide a good starting point with regard to the integration of operational resilience requirements and processes.

Delivering BAU

6. Assess operational resilience of critical services end-to-end

This is where the effort around creating an effective operating model for operational resilience pays off. Based on assessments of criticality and focus, the function should then look to apply resilience skill and practices over these processes. Mapping critical products or services end to end, including all interactions with the customer enables a seamless view of the process and is more intuitive in comparison to a functional view. Operational resilience is an issue that is best viewed from a customer, client or market perspective as it is in those spheres that the impacts of an outage or issue are most keenly felt.

Further mapping of dependencies across the four pillars, or resource enablers, of people, technology, premises and third parties enables you to gain a complete view of the process and the underlying facilitative disciplines. Identifying the critical points of failure and the mitigating controls requires input from a range of subject matter experts. Once identified, the level of risk exposure can be identified and validated. In some cases, organisations may have key controls identified as part of an ERM, Operational or Compliance Risk system, which can add valuable insight to the analysis.



A fundamental aspect of this approach is the change in perspective of those participating in the delivery of the service or product. Handovers between the business, functions and with the customer need to be clearly understood and responsibility should be taken on both sides for ensuring they are seamless. Rather than merely being the 'front end' of the service, the business is now seen as holding ultimate responsibility for the end to end process.

7. Remediate resilience gaps

As a consequence of a rigorous and robust mapping of processes and identification of key controls, a programme of work will likely be required to remediate gaps or to enhance the overall processes' resilience. This should be coordinated and executed by first line teams with the support of operational resilience specialists. Decisions on investment for mitigation or for risk acceptance should be made at a service level by the business through consultation with the underlying functions involved in providing the service.

What does a sustainable operational resilience function look like?

While operational resilience outcomes are the responsibility of management, service owners and risk owners, we think there should be a central point of responsibility and ownership for the operational resilience framework. We suggest that this function is not a virtual team, which may not be sustainable due to competing priorities and reporting lines, but a dedicated first line function where the business as usual resilience programme can be anchored. A programme that operates within the first line with second line oversight would likely be an effective dynamic in delivering resilience. Cohesion and coordination is crucial to successfully delivering resilience outcomes, especially in large complex organisations.

As previously mentioned, there is a natural home for resilience within existing business continuity teams with SMF 24 ownership. Increasingly, we are also seeing organisations align their operational resilience function with security functions, including cyber security.

One of the most important parts of the operational resilience programme is the relation of risk data to end to end critical services. The operational resilience function will be users or recipients of data from many different sources, but they will own very few data resource themselves (with the possible exceptions of business continuity and service continuity). With its expanded remit and activities not previously covered by business continuity functions, there is a need to address the type of skills and capabilities that the operational resilience function requires to meet its objectives and to be effective.

'Business continuity practitioners possess many, but not all, of the knowledge and skills that are necessary to help organisations to develop and enhance resilience capabilities. It is unlikely that a single person in any organisation will possess the necessary knowledge and skills to implement and deliver all resilience objectives. The development and enhancement of organisational resilience capabilities will require a collaborative effort between participants across many management disciplines.' ***'Organisational resilience – BCI position statement – February 2016.***

Teams should be expanded to include people with a detailed understanding of the business and customer journeys. Let's therefore assume that a resilience function requires different skill sets and capabilities when compared to a traditional business continuity management (BCM) or IT disaster recovery (ITDR) team. This assumption leads us to a number of questions: how are the skills and capabilities required in the resilience different? How can you identify these differences and ensure that the skills that are added to the team are those that will best serve your organisation? How far is your BCM or ITDR function currently from the resource profile you have identified for resilience?

How a resilience function may look

In our view, organisations should consider widening the resource pool from which to recruit for operational resilience beyond BCM specialists. In building your function, you should seek expertise and knowledge across the four pillars of operational resilience - people, technology, third parties, premises. This is particularly true in areas with highly complex interdependencies such as clearing services and investment banking. A more detailed understanding of what operational resilience teams need to protect will help better direct resources and effort. By doing this, you will make the function more attractive to potential recruits as the roles are more varied and require transferable skills, such as data analytics. Such roles can potentially lead to more varied career paths and opportunities than those associated with a traditional BCM function. We outline below some of the attributes we would expect to see in an organisation that demonstrates a broader operational resilience capability:

Resilience business partners

Front-line business-facing consultants who are responsible for the delivery of the resilience risk service to senior leaders and critical functions/processes. This role requires individuals who have either business or technical expertise.

Resilience centre of excellence

Subject matter expert teams within the resilience function that provide broad support underpinning the whole programme; such as the central governance and reporting team, change, and tooling.

Resilience service providers

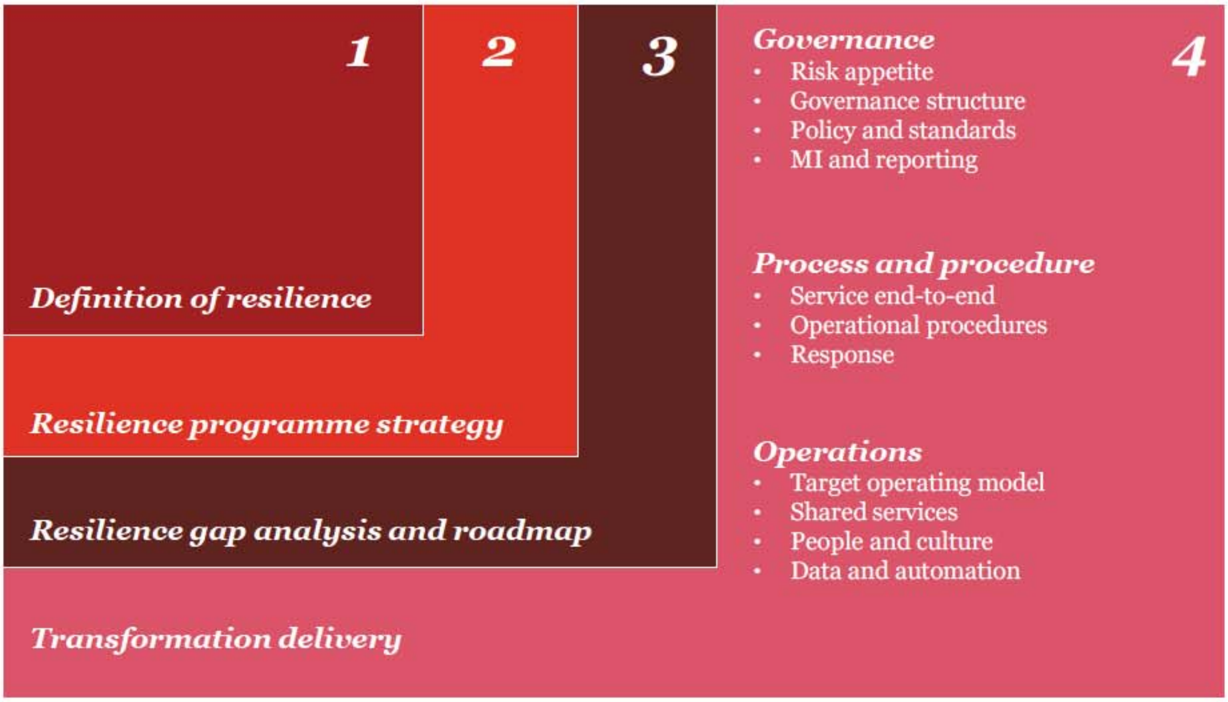
Operational delivery of recovery and crisis programme to non-critical business areas. Supporting the all areas of the resilience function through delivery of standardised repeatable processes, including data mining and user support.

Resilience technical delivery

These teams directly support the front-line resilience business partners in delivery of the resilience programme. Providing technical specialisms including crisis management, testing (business and ITDR) and resilience discipline knowledge i.e. technology, third parties and premises.

Treat it is a transformational change:

If you are seeking to make a step change in your approach to operational resilience, it is likely to feel more like a transformation programme than an enhancement to an existing capability. Given the current environment, elevating the profile of your programme of work in operational resilience can be transformative for your entire organisation, not just those immediately involved in the function. Outlined below is an indication of the important elements of a resilience transformation programme, from establishing the definition to considering policies and procedures.



1

Definition of resilience

2

Resilience programme strategy

3

Resilience gap analysis and roadmap

4

Governance

- Risk appetite
- Governance structure
- Policy and standards
- MI and reporting

Process and procedure

- Service end-to-end
- Operational procedures
- Response

Operations

- Target operating model
- Shared services
- People and culture
- Data and automation

Transformation delivery

Common pitfalls in making change:

Don't reinvent the wheel

You will already have many of the component parts of the framework, so use these as a foundation to grow your capability. Value comes from bringing these components together, working to a common strategy and integrating their risk indicators in to your resilience programme in a coordinated manner.

Take the customer view

Regulatory focus, technological advances and evolving business practices have placed the customer or client firmly at the centre of resilience strategies. Defining and embedding ownership of top level customer or client services to drive the resilience agenda is a key challenge for leaders across the sector.

Get the complete picture

Understand the end to end processes that underpin the customer or client service. This is a key element of the business analysis required to relate resilience risk and investment decisions back to both critical economic functions and customer impact.

Measure resilience risk

To obtain a complete view of resilience, risk data sources and key risk indicators must cover a broad range of disciplines. Identifying, relating and reporting of resilience KRIs, in a manner which enables stakeholders to see resilience risk performance and trends clearly presented, is increasingly important.

4. Extensions of operational resilience

“Embrace incidents and use them as learning opportunities rather than hide from them.”

– Director of Group IT, Security and People Risk at major UK retail bank

Chapter summary:

Disciplines outside of the traditional operational technology areas are now becoming more intertwined with operational resilience. We outline in the section below some examples, including cyber security and outsourcing risk, as they can be addressed by an effective operational resilience capability.

Cyber resilience

‘Cyber-attacks in the financial services sector are becoming more frequent and widespread. This is potentially made worse by the use of complex and ageing IT systems, outsourcing of operations and the growing transfer of data between firms.’ FCA Business Plan 2018/19.

The environment

The frequency and sophistication of cyber-attacks is increasing, with the number of material attacks reported to the FCA up by more than 80% in 2017. Attackers are moving up the value chain, seeking bigger gains while making more substantial investments, making the financial services industry a top target. The UK industry is categorised as national critical infrastructure making it a target for increasingly advanced and hostile national cyber capabilities. So called ‘hacktavist’ organisations are increasingly targeting the industry, which they see as a catalyst for social inequality and corruption.

The number of internet enabled devices, many of which are unsecured, has risen by almost 25% in the last two years to over 20bn. With the evolution of the ‘internet of things’ this number is forecast to grow to 75 billion by 2025. Advances in artificial intelligence technology have made it easier for criminal organisations to take control of large ‘botnets’, with the largest controlling millions of devices, exponentially increasing the potential power of attacks.

The issues

Like technology incidents, cyber breaches can cause significant disruption to critical economic functions (CEFs) and undermine customer trust. Customers have high expectations around the security of their data with no accidental exposure being deemed acceptable. As financial services business models become increasingly dependent on new technologies and processes, firms should ensure they manage the risks new systems bring.

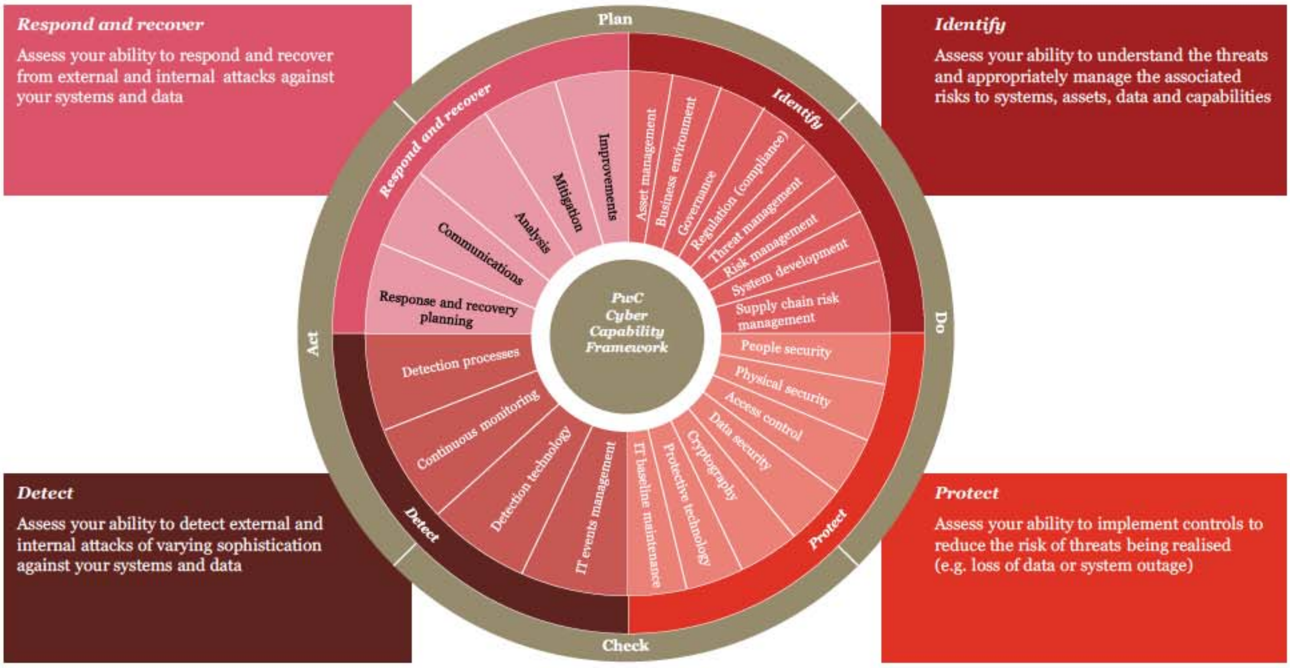
Denial of service (DoS) attacks are one of the most common cyber-attacks impacting financial services institutions. DoS attacks are designed to shut down machines or networks by flooding the target with traffic making them unavailable to intended users. Over the last few years HSBC, Lloyds and RBS have all been victims of DoS attacks with disruption lasting up to 48 hours.

No combination of security controls can guarantee immunity from cyber-attack, but financial services firms should ensure that they take adequate steps to limit the likelihood and impact of attacks on their organisation. Cyber resilience is an approach that builds on the foundations set out by conventional approaches to defining a cyber security strategy.

Current responses

'While most financial services firms have dedicated a growing amount of attention and resource to securing their estate, they need to ensure that they stay ahead of the rapidly developing threats. Many organisations have established a complete set of security capabilities based on known frameworks (e.g. NIST) and have invested in getting the lagging capabilities up to a desired state. But many will not have considered the maturity of their response and the activities that are necessary following a breach.

An effective approach to cyber resilience allows you to enhance your approach to managing threats by aligning activities to CEFs. It requires involving business stakeholders in the security activities and stress-testing of critical controls.



Respond and recover

Assess your ability to respond and recover from external and internal attacks against your systems and data

Identify

Assess your ability to understand the threats and appropriately manage the associated risks to systems, assets, data and capabilities

Detect

Assess your ability to detect external and internal attacks of varying sophistication against your systems and data

Protect

Assess your ability to implement controls to reduce the risk of threats being realised (e.g. loss of data or system outage)

'While cyber risks should be managed as part of an FMIs' (organisations) overall operational risk management framework, some unique characteristics of cyber risk present challenges to FMIs' (organisations) traditional risks management frameworks.' – *Committee on Payments and Market Infrastructures and Board of the International Organisation of Securities Commissions Guidance on cyber resilience for financial market infrastructures Guidance on cyber resilience for financial market infrastructures*.

Outsourcing

The environment

Financial services firms are increasingly seeking to outsource critical functions to a concentrated set of vendors to reduce cost and gain access to capabilities not readily available to the industry. Growing outsourcing, especially in emerging technologies, makes it harder for firms to quantify and manage their third party risk.

While regulators allow firms to outsource critical functions, they will hold senior management to account over the actions of their third party service providers. Regulatory pressure is continuing to grow with the FCA and European Central Bank (ECB) identifying outsourcing risk as a key area of focus in 2018/19. The ECB and European Banking Authority (EBA) have launched a thematic review of outsourcing supervision across the EU with the view to publish a standardised set of requirements. GDPR also places additional due diligence onus on outsourcing providers to ensure that vendors have adequate security controls.

The issues

Failures at third parties can result in significant disruption and can undermine the security of the outsourcing firm as controls are bypassed through the targeting of vendors. The interconnectedness of the financial services industry means that localised outages can quickly become contagious. There is potential for global issues to develop, especially where multiple firms depend on the same service provider.

As a result of the escalating risk, board level executives are increasingly focusing on outsourcing practices. In most cases, this has not translated into clear accountability which often results in no-one having a holistic overview of who the firm is doing business with and the associated risks.

Current responses

The current approach to vendor management and supplier risk is often siloed with individual teams focusing on different areas. While organisations are right to be proactive, they should ensure that their approach is joined up. To gain visibility across the vendor landscape firms should consider procuring a centralised tool (e.g. Know Your Third Party by IHS Markit) and integrate across all relevant capabilities.

Firms need to ensure that they retain appropriate oversight of third party providers and take responsibility for the service they provide. Doing so will reduce the risk of outages and accidental information disclosure. To do this, you should keep a comprehensive, accurate list of all outsourced service providers detailing the procured services, partners, roles and responsibilities and any contractual obligations. You should use this comprehensive list of third party services to produce a catalogue of risks associated with the outsourced services. You can then categorise vendors into risk bands depending on criticality and level of risk.

Operational continuity in resolution (OCIR)

OCIR is part of a broader set of recovery and resolution planning (RRP) requirements from the PRA. It aims to ensure that services, whether provided from within the same entity, from another group entity or from an external supplier which support the CEF, continue in recovery and resolution. Firms must demonstrate how the OCIR arrangements it puts in place are aligned to its recovery options and resolution strategy. OCIR applies to large and mid-sized banks which provide critical functions in the UK and meet certain financial thresholds.

Although there are similarities, the objectives and context of operational resilience are different from operational continuity. Operational resilience is an outcome that is achieved in BAU as well as recovery and resolution. Operational continuity is an outcome which is achieved in recovery or resolution, although the objective is somewhat achieved through arrangements in place in BAU which support that objective. Some key points of difference are:

- OCIR focuses on firms' CEFs and ensuring they can operationally continue in spite of financial distress and actions taken in recovery or resolution to restructure an entity or group.
- OCIR focuses on supporting the firm through the period leading up to resolution or to facilitate an orderly wind down.
- When considering OCIR, the interconnectedness and complexity of firms (e.g. lack of clarity on service recipients, charging structures, ownership of assets, location of key staff) are significant barriers firms must overcome when developing plans.

Despite these differences, it is important to recognise there are synergies between operational continuity and operational resilience. In particular the service mapping of CEFs, critical resilience functions (underlying people, assets, systems, data, infrastructure, vendors) and processes to maintain this data and your ability to report on the current state of resilience on an ongoing basis are points of consistency. Both disciplines also highlight the need to identify clear ownership and responsibility within a firm.

5. Regulatory supervision and enforcement

“The take-up of technology and innovation across and between firms is accelerating creating a conveyor belt of risks and opportunities.”

– Andrew Bailey (Chief Executive FCA)

Chapter summary

Whilst much of this paper has focused on the business outcomes of developing your operational resilience function, regulatory compliance remains a major driver. Consumers increasing dependence on technology solutions and the resulting harm when things go wrong has led regulators to take an increasingly hard line approach to operational resilience. Both the FCA’s and PRA’s latest business plans continue to list operational and cyber resilience as key focus areas indicating that regulatory action will continue to increase in this space.

UK

In the UK, the FCA identified technology resilience and information security as cross-sector areas of focus in its seven most recent annual business plans. Likewise, operational resilience has been an increasingly prominent feature of the PRA’s agenda.

UK regulators are using data to benchmark firms against their peers with ‘SpotCheck’ and resilience questionnaires sent to a range of firms. In some cases, the responses to these has resulted in follow-up supervisory action. The statistics arising from these exercises are likely to play an increasingly important role in firm end of year reviews.

The PRA defines a list of ‘CEFs’ and is publishing a discussion paper outlining a set of standards imminently. Its approach goes further than business continuity (recovering from an incident) and focuses heavily on designing IT systems to withstand or minimise the risks of disruptive events. Increasingly proactive micro-supervisory interventions, such as the ‘Dear Chairman’ exercises and CBEST testing, are being deployed to set expectations and assess against them.

Cyber-attacks in the UK are becoming increasingly common and the financial services industry is a particular target. Regulators are working closely with the Government, the National Crime Agency, National Cyber Security Centre and HM Treasury to assess the capabilities of individual firms and to attempt to minimise the impact of breaches on consumers and the industry.

The FCA and PRA say that they will continue to develop regulatory tools to better assess firms and identify where harm could occur, so firms should expect to be required to interact with the regulators on an ongoing basis on this issue.

In the near-term, the BoE’s Financial Policy Committee (FPC) has announced the introduction of impact tolerances and stress testing for the delivery of vital services that the financial system provides to the economy. The BoE plans to set out clear expectations and a testing regime for how quickly firms will be able to recover from a cyber incident. The initial focus will be on payments and derivatives trading. The pilot of stress testing approach will commence in 2019.

To date regulatory investigations and subsequent enforcement action have predominantly focused on large, systemically important banks where even small outages can cause widespread disruption, but the as the industry increasingly adopts new technologies and innovation, regulators are likely to increase the scope of their reviews to a broader range of firms. The FCA’s 2018/19 Business Plan identifies ‘cyber and technological risk' as a key cross-sector issue and the FCA states that it will 'conduct focused thematic work with lower impact firms', based on harms it has identified in each sector.

Europe

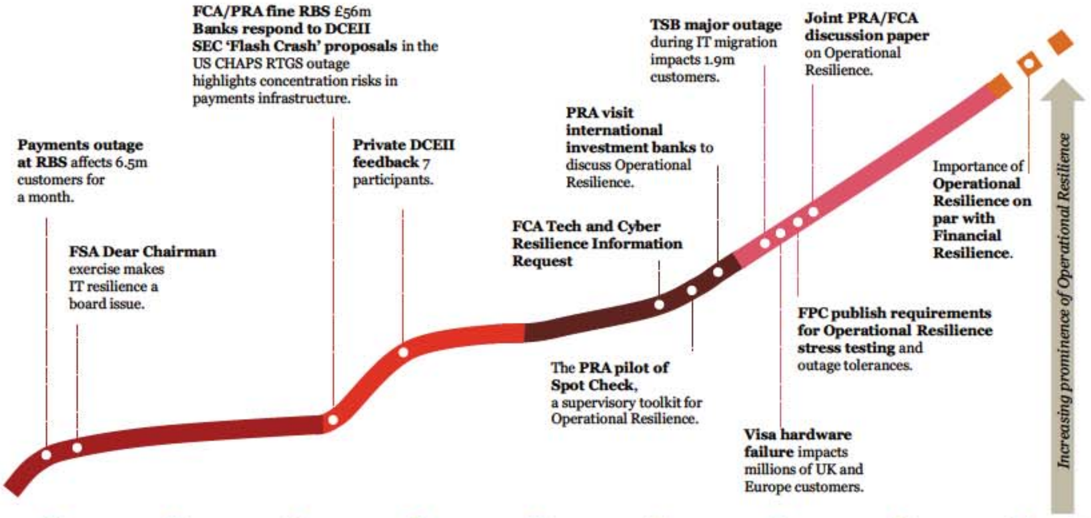
Operational resilience is also high on the priority list for regulators across Europe, both for the EU Supervisory Authorities (ESAs) and national competent authorities (NCAs). Historically, there has been limited harmonisation at the pan-EU level of operational resilience regulation. This has resulted in differing supervisory approaches being developed across the EU to deal with the potential risks. While some localised standard-setting is appropriate given differences in landscapes, this divergence has led to international firms having to comply with varying sets of standards and guidelines. More recently, European regulators have focused on converging regulation and supervisory practices in order to promote greater consistency of approach.

This has been driven by the increasing use of technology by firms, including on a cross border, and its implications for effective prudential and operational supervision.

In line with their mission to create a standardised EU 'Single Rulebook', the ESAs have focused on detailing technology and operational resilience standards in recent European-wide regulation. Key components of this are the Markets in Financial Derivatives Directive II (MiFID II) and the Payment Service Directive II (PSD II).

To underpin legislative changes, the ESAs are releasing guidance to both NCAs and firms outlining their expectations. For example, the EBA released guidance on cloud outsourcing in December 2017. Both the EBA and ECB are conducting a thematic review on outsourcing and associated IT risks over the course of 2018. Based on best practices identified in banks, this guidance will present supervisory expectations in terms of 'outsourcing arrangements, risk management, governance and monitoring, and will address the procedures followed and engagement with the supervisor'. Overall, the guidance is expected to aim to clarify and operationalise expectations with respect to banks' management of outsourcing, harmonising standards for significant institutions.

On top of the regulation and guidance published by European bodies, NCAs are becoming increasingly vocal over their expected operational resilience standards. FINMA (Switzerland), the AMF (France) and BaFIN (Germany) have all listed technology and cyber resilience as a key priority for the coming years. The AMF plans to develop new expertise to address emerging risks in particular, for cybersecurity and, in general, regarding the robustness of IT systems. BaFIN has published 'Bankaufsichtliche Anforderungen an die IT' (BAIT) which offers clarity to management boards of institutions on banking supervisors' expectations with regard to 'the secure design of IT systems and associated processes, as well as on the relevant requirements placed on IT governance'. It's clear that firms can expect to see further activity from NCAs, both through formal guidance and supervisory activity – we explore this in the following chapter.


FCA/PRA fine RBS £56m
Banks respond to DCEII
SEC 'Flash Crash' proposals in the US CHAPS RTGS outage highlights concentration risks in payments infrastructure.
Payments outage at RBS affects 6.5m customers for a month.
FSA Dear Chairman exercise makes IT resilience a board issue.
Private DCEII feedback 7 participants.
PRA visit international investment banks to discuss Operational Resilience.
FCA Tech and Cyber Resilience Information Request
The PRA pilot of Spot Check, a supervisory toolkit for Operational Resilience.
TSB major outage during IT migration impacts 1.9m customers.
Joint PRA/FCA discussion paper on Operational Resilience.
Visa hardware failure impacts millions of UK and Europe customers.
FPC publish requirements for Operational Resilience stress testing and outage tolerances.
Importance of Operational Resilience on par with Financial Resilience.
Increasing prominence of Operational Resilience
2012
2013
2014
2015
2016
2017
2018
2019
2020

6. The future of operational resilience

“Control and real time monitoring allows the business to adapt quicker with confidence.”

– Head of Resilience and Continuity at major multi-sector bank

Chapter summary:

Approaches to operational resilience are going to develop quickly over the coming years, and keeping abreast of this developing discipline is critical for organisations. While operational risk related practices have developed over time, an increasing reliance on complex technology and infrastructures has intensified the risk of operational failure. To build consumer trust, make smarter investment decisions, comply with an increasingly prescriptive regulatory regime and change with confidence, firms should be looking to advancing technology to provide actionable data to decision makers and fostering a ‘resilient culture’ throughout the organisation.

Many of the developments that will impact operational resilience over the next decade are somewhat unpredictable and intrinsically linked to technological advancements, but we have identified five key trends to help form a picture of what the future of operational resilience could look like in the future.

Continued expansion of regulation and increased supervision

The chief executives of both the PRA and FCA highlighted operational resilience as a key priority in the forewords of their 2018/19 business plans. This sentiment is echoed by European regulators who have identified operational incidents as a threat to financial stability. Recent European regulation, such as PSD II and MiFID II, have imposed stronger operational requirements on firms.

To date the majority of regulatory activity relating to resilience has focused on the banking sector. However, the FCA and PRA have indicated that the scope of their supervisory activity will expand to focus more heavily on the insurance and asset and wealth management sectors. Significantly, the PRA is planning to produce the first overarching prudential standard for operational resilience in the world. This will include identifying firms where an operational failure could have a significant impact on the real economy and considering the level of resilience that regulators expect firms to demonstrate.

These developments are likely to come to fruition over the next 12 to 18 months, but the broader trend of increased regulatory scrutiny is likely to continue beyond this period. In a world increasingly reliant on financial services and with innovation and technological advancement driving the market, regulators will need to ensure their efforts keep pace with developments.

Public sensitivity to operational outages has increased, with even small outages garnering a lot of attention in the press and on social media. High profile outages, such as the recent migration failure at a large UK bank and the cyber-style raid of a mid-size UK bank, have highlighted to consumers, firms and regulators the potential consumer harm resulting from operational incidents. As a result of this, it is likely that over the coming years we will see regulators impose tighter rules of engagement on firms across the financial service industry.

Improved data and analytics

Computing power has doubled annually since the 1970s and the cost of processing data has dropped at a similar rate. Enhanced capability and reduced cost has allowed data analytics to transform all aspects of life including the financial services industry. Enhanced digitisation, data governance and the adoption of emerging technology has given firms access to more data than ever before.

Providing a detailed view of operational risks across an organisation is a key role of the operational resilience team, however, the data currently presented is backward looking and hard to interpret. For operational resilience teams to proactively manage the rapidly changing risk landscape they need to make better use of the data held by their firm to make near real-time decisions.

A good example is capacity management. To ensure the continuity of critical functions, financial services firms need to predict the required capacity of their systems. The current approach at many firms is to run systems with ample headroom to allow for spikes in users – but this can require substantial computing and financial resources.

System use is impacted by a number of variables including marketing campaigns and the time of the year, but is predictable with the right data. Enhanced data analytics would allow operational resilience teams to incorporate business data with system logs to proactively anticipate required capacity. Combine this data with artificial intelligence technology and cloud infrastructure and firms will be able to automatically vary their computing power in real-time to such that it is created or reduced as required.

Enhanced data analytics stands to be a game changer in this field. Many organisations are setting up sandboxes to look for innovative products. While firms are making progress, many operational risk data analytics initiatives remain immature. Taking advantage of new data and processing techniques will enable operational resilience functions to report meaningful and comparable metrics to senior management. In turn, this will allow them to make better risk management decisions and capitalise on risk taking opportunities in a controlled way.

Fostering innovation

As operational resilience capabilities develop, it will be increasingly important that they contain the right skill sets to support the business. A function that is strategically minded and positions itself on the front foot in working with the business will be better able to support innovation and enable in new offerings.

Historically, criticism has been levelled at control functions concerning their ability to move with the business. The more closely the operational resilience capability can operate with the business, the better. If they are able to forecast anticipated business need and risks, their value to the organisation will increase significantly.

Becoming fearless

Building, or indeed maintaining, customer trust should be a key objective of any operational resilience team. To date, operational resilience teams have focused on minimising the likelihood and impact of incidents, but as one Head of Resilience we interviewed puts it: ‘outages are inevitable’. While a small subset of users are likely to be unreasonable when incidents occur, many understand that outages are a part of modern day financial services. How a firm responds to incidents can differentiate them from their competition and can define how long consumers hold on to any adverse feelings.

The rise of social media and increased coverage of the press has instilled a fear of incidents into many CIOs, COOs, CROs and heads of operational risk. This has led to many firms trying to cover up incidents by publishing limited information. At times this fear has also led to weakened internal governance as teams bypass controls to get their firm operational as quickly as possible. In a world where operational incidents are inevitable, operational risk teams should be working with IT and business teams to develop robust incident response procedures that go beyond traditional business continuity or disaster recovery.

Having a positive response to customers when something goes wrong is key to managing the external perception of the incident and its impact. This works well when a firm’s response contains three things: First, a sincere admission of guilt and responsibility. Second, a detailed description of what went wrong and how they are going to avoid the issue in the future. Third, some kind of compensation commensurate to the level of inconvenience caused. When determining your incident response, you should look outside the industry for examples of great customer service. Doing so could in fact allow you to profit from incidents as it gives you a platform to show that you really understand and care about your customers, turning a crisis into an opportunity.

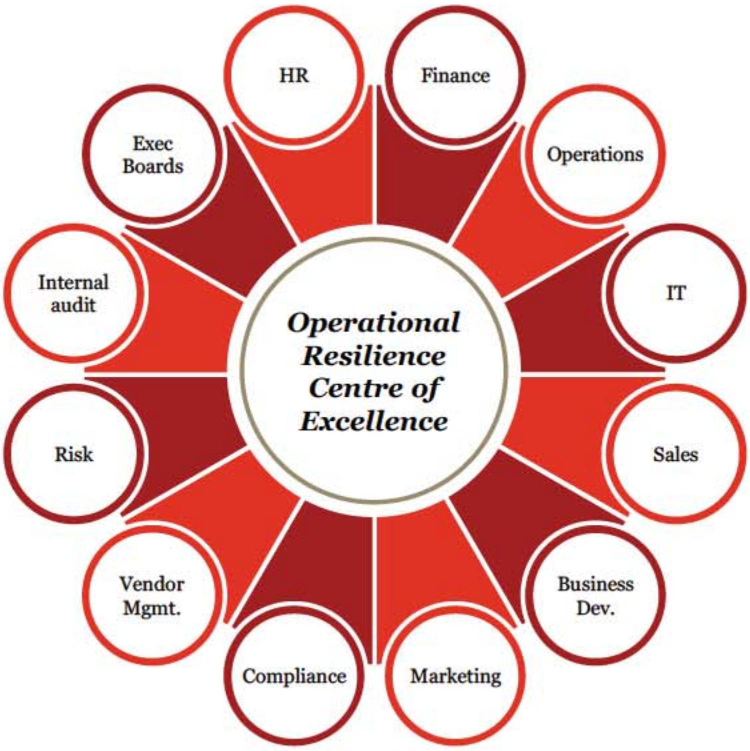
In 1993, Pepsi sales sunk by 2% as reports emerged of a syringe being found in a can. The following week there were 50 other reports of can tampering. The reports turned out to be fraudulent but were believed by a large subset of the public and media. Although confident in their processes, Pepsi's response did not contain vague assurances to trust them. They set out to change consumer perceptions by publishing four videos including a detailed review of their canning process.

The approach of publishing detailed explanations of incidents has been taken up by some FinTech firms, many of whom see customer service as their key USP. One firm has gone to great lengths to describe often complicated incidents in an easily understood but comprehensive way. The firm details the cause of the outage, explaining the technology and dependencies. Importantly, they detail what measures they took to ensure that it doesn't reoccur in the future. One detailed incident report prompted a customer to comment 'whilst the cards being down is an inconvenience I have to say that the level of interaction and communication with the customer base has been outstanding, still head and shoulders above my high street account.'

Cultivating a strong culture

Recent regulatory action has elevated operational resilience to a position of high priority on the boards of financial services firms. But risk teams and executives cannot control operational risks on their own and need to foster a strong operational resilience culture throughout the firm. To maximise efficiency and spread cost across multiple business units, we are increasingly seeing operational resilience functions employing a centre of excellence model with representatives throughout the business.

Under the centre of excellence model, the operational resilience team sits at the hub and acts as a point of contact outlining best practice and direction. Each business unit throughout the organisation will assign their own operational resilience representative(s) with a number of dedicated hours dictated by the risk and criticality of the function. 'This model gives us further reach into the business whilst spreading the cost'.



We worked with London First in 2016 to learn more about how the topic of 'organisational resilience' was perceived in industry. We also set out to establish the level of resilience leaders and managers believe their organisations to have. A key finding of our report was that culture and strategy are as important as risk management, business continuity and other disciplines in ensuring operational resilience. Our research found that 92% of leaders believe that culture plays a vital role in organisational resilience.

Diversify the delivery model

As we have seen, current resilience teams may not have all the skills needed in the future. The operational resilience capability needs to ensure that their skill sets reflect the changing risk landscape and need to ensure that the team is refreshed with new skills as they become relevant. However, as one Head of Operational Resilience puts it ‘everyone is after the same people’ so to solve the problem of a potentially limited resource pool and the unrelenting pressure to do more with less, resilience leaders will need to consider alternative operating models.

Developing a service catalogue and delivery approach based on criticality can help to focus time, effort, resource and budget on what must be protected. The areas of your organisation, which are categorised as less critical, may then lend themselves to follow a standard, repeatable and lower cost model for managing resilience risk. Leaders should examine ways in which they can augment their capabilities, whilst retaining deep knowledge based in situ with the critical business teams, delivery of support services can be achieved through an offshore or nearshore managed service model.

How we help our clients

> “Failures to core systems undermine confidence in financial institutions and are detrimental to customer outcomes and market integrity. As complexity and connectivity increases, so does risk. We help businesses understand, identify and manage these technology risk exposures, the impact to critical functions, and business interactions with markets and customers.”
>
> – Simon Chard, Partner, Financial Services Technology and Operational Resilience Practice

Chapter summary:

In 2012, PwC created a dedicated Financial Services operational resilience practice in response to the incident at RBS. To help firms capitalise on business benefits and exceed regulatory expectations we have built a portfolio of risk, resilience and change solutions that are proven in action and deliver real-world, practical benefits. Our highly specialised team have worked across the industry to assure and develop firm’s operational resilience and have experience working in retail and investment banks, with regulators and FMIs and across the insurance and wealth management sectors.

In 2012, PwC created a dedicated financial services operational resilience practice which has helped firms of all sizes to meet regulatory expectations and capitalise of the business benefits of having a highly resilient organisation. Our bespoke Operational Resilience Maturity Assessment (ORMA) framework has been used to help benchmark firms of all sizes throughout the UK financial services industry and abroad. It has been adapted to reflect the latest regulatory thinking, including the PRA’s latest SpotCheck questionnaire. The assessment baselines a firm’s current maturity against industry best practice and regulatory requirements and produces a list of prioritised, recommendations.

We help organisations become more resilient and risk intelligent – focusing their efforts on what matters most to their customers, market and their shareholders, leveraging data and technology to improve risk and control coverage, effectiveness and efficiency. We have worked with over 40 clients across the breadth of financial services ranging from retail and investment banks to regulators and critical financial infrastructure as well as wealth managers and insurers. Our core services include but are not limited to:

Our services and approach

1 Business Case for focus on Operational Resilience

2 Operational Resilience Maturity Assessment

3 Regulatory Response

4 Programme Development and Support

5 Board Reporting and SMF Support

6 Assure your response

7 Testing

8 Managed Service

	Activities	*How we can support you*
1. Business case for focus on Operational resilience	Getting a clear Board mandate at the start of your operational resilience journey will embed senior buy-in and ownership from the start.	• Translating regulatory expectations into operational requirements. • Resilience definition and strategy.
2. Operational Resilience Maturity Assessment	Understanding your current level of maturity against regulatory expectations allows you to develop a roadmap for improvement.	• Perform a current state maturity assessment of your resilience capability. • Develop an actionable roadmap to improve your maturity.
3. Regulatory response	With the increased regulatory focus, it is likely that you will need to respond to more questions and assessments from the regulator.	• Stress testing rehearsal / dry run. • Benchmarking of stress testing tolerances and performance. • Post Incident Review & Root Cause Analysis.
4. Programme development and support	The delivery of your operational resilience plan, often starting as a project, but needing to transition into BAU as it becomes embedded.	• Target operating models and development of your book of work. • Risk appetite and criticality definition. • Mapping and assessment of end-to-end service resilience and delivery capabilities. • Tools and automation. • Training and awareness. • Policies and standards. • Governance and control frameworks. • Process and procedures. • Crisis response frameworks.
5. Board Reporting and SMF Support	Regular, demonstrable, reporting to Board and committees.	• MI and reporting, including KPIs and KRIs. • Governance structures. • SMF briefings and training • Technology and business risk alignment. • Crisis management planning.
6. Assure your response	Assurance of your remediation is critical to ensuring the delivery of the change you need in order to develop resilience capability.	• Quality closure. • Programme and Project management.

	Activities	*How we can support you*
7. Testing	Your ability to prove your resilience capabilities to stakeholders and to identify areas for remediation.	• Crisis exercise / simulation. • IT Disaster Recovery design and support. • Business recovery desktop exercising. • Stress testing rehearsal / dry run.
8. Managed Service	Consideration of outsourcing routine internal resilience processes to a PwC in order to allow your operational resilience team to focus on critical services.	• Support the delivery of routine resilience services including BIA and BCP completion and report production.

Value to our clients

In delivering the services outlined above, we provide the following value and benefits to our clients:

Focused investment and reduced costs

Keeping control of the narrative with Board and Regulators

Becoming more Risk Intelligent through focus and technology enablement

Clarity over regulatory expectations

Confidence and trust in Technology risk capabilities and knowing they are in control

Future-proofing of capabilities

Greater assurance

Stronger organisational understanding of resilience

Developing a stronger resilience culture

Contributors

Simon Chard
Financial Services, Technology Assurance
Partner
☎ : 07740 241 051
💻 : simon.c.chard@pwc.com

Duncan Scott
Financial Services Risk and Regulation
Director
☎ : 07894 393 607
💻 : duncan.j.scott@pwc.com

Glenn Gurney
Financial Services, Commercial Assurance
Director
☎ : 07725 633 144
💻 : glenn.gurney@pwc.com

Paul Marsden
Financial Services IT and Operational Resilience
Senior Manager
☎ : 07803 455 547
💻 : paul.marsden@pwc.com

Luke Nelson
Financial Services Risk and Regulation
Senior Manager
☎ : 07808 107 043
💻 : luke.a.nelson@pwc.com

David Lukeman
Financial Services, Technology Assurance
Partner
☎ : 07801 227 259
💻 : david.lukeman@pwc.com

Stella Nunn
Financial Services IT and Operational Resilience
Director
☎ : 07932 144 627
💻 : stella.nunn@pwc.com

Christian Arndt
Financial Services Cyber Security
Technical Fellow
☎ : 07760 400 335
💻 : christian.arndt@pwc.com

Lewis McKenzie
Financial Services IT and Operational Resilience
Senior Manager
☎ : 07843 330 123
💻 : lewis.mckenzie@pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

180703-164201-DS-OS