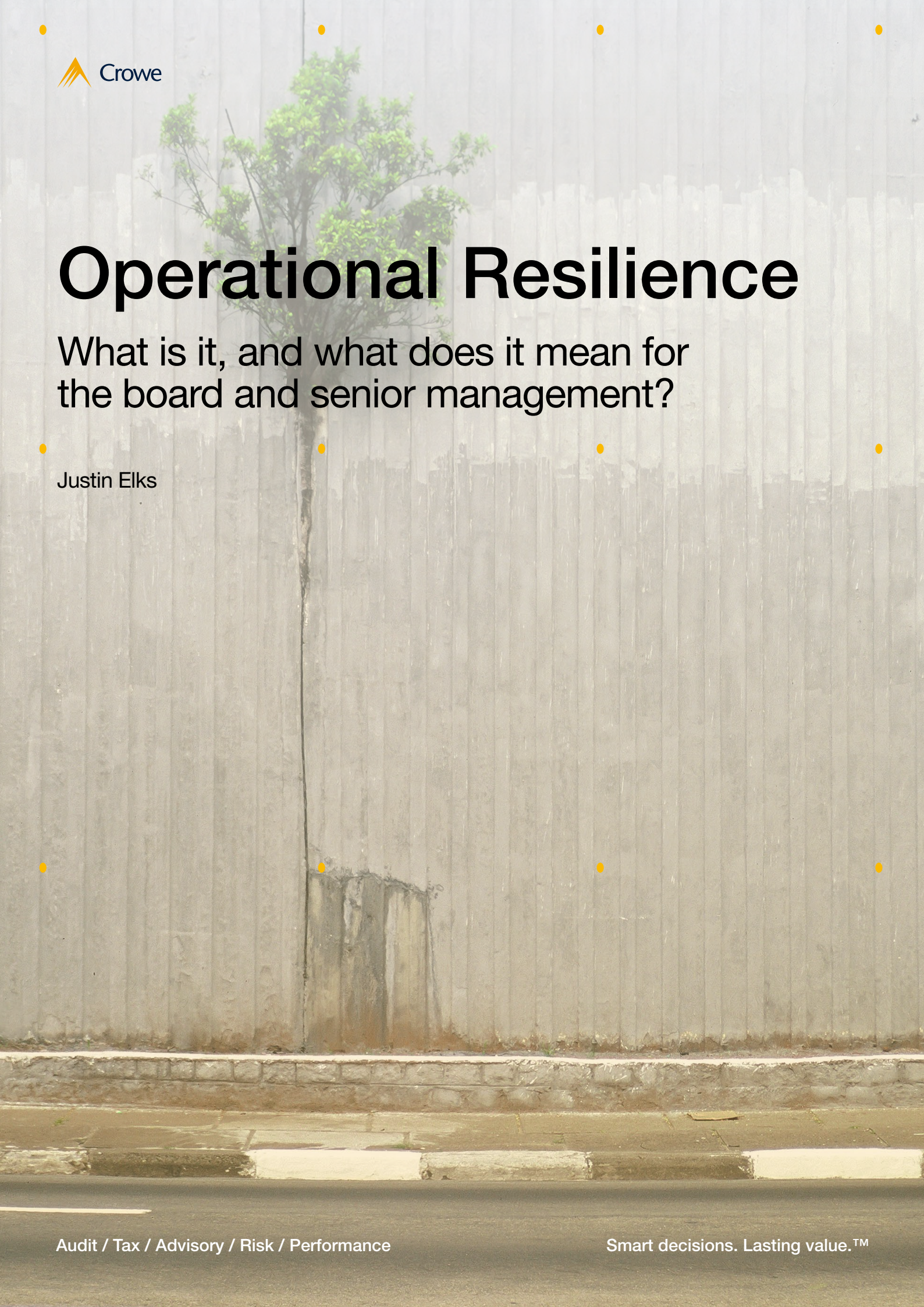


Crowe

Operational Resilience

What is it, and what does it mean for the board and senior management?

Justin Elks

Executive Summary

1. What is operational resilience?

Operational resilience is the ability of a company to build confidence and trust in its capability to adapt to changing circumstances. This is achieved by preventing, responding to, and recovering and learning from stresses and disruptions whilst delivering on promises to customers, achieving critical business objectives, and operating within agreed tolerances.

2. Requirements of proposed UK regulation

Regulators in the UK are taking a strong and consistent approach to increase resilience across the financial services sector to ensure that it can continue to provide key services, with only limited interruption, when faced with severe but plausible operational events. They require companies to prioritise the things that matter, set clear standards and invest to build resilience.

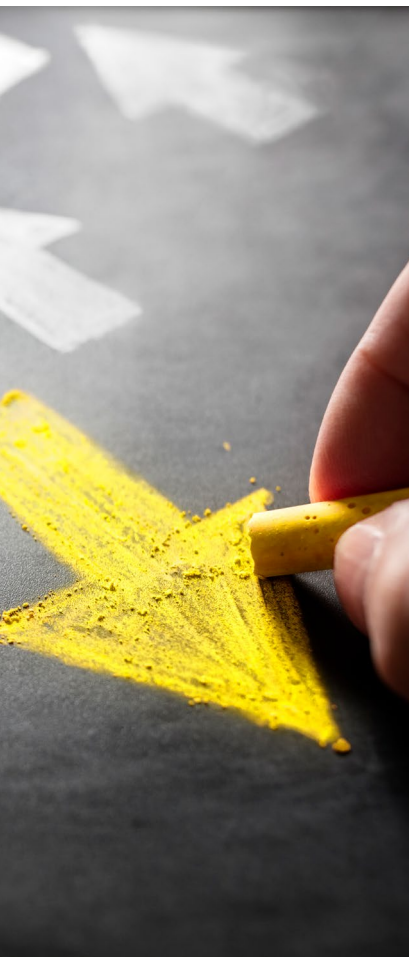
Firms need to:

- **Identify their important business services** that if disrupted could cause harm to consumers or market integrity, threaten the viability of firms and their safety and soundness or cause instability in the financial system.
- **Set impact tolerances** for each important business service, with clear metrics which clearly quantify the maximum level of disruption they would tolerate.
- **Identify and map the chain of resources** that support their delivery of important business services.
- **Take actions to be able to remain within their impact tolerances** under a range of severe but plausible disruption scenarios.
- Complete a regular **self-assessment** to demonstrate compliance.

Regulators expect companies to focus beyond the boundaries of their own firms, to consider the needs of the people and organisations that depend on them to deliver, as well as ensuring that they apply the same level of operational resilience to in-house and outsourced processes and functions.

Boards are expected to play a critical role in setting and overseeing the implementation of a firm's approach to operational resilience. Where it exists, the Chief Operations role, Senior Management Function (SMF24), is responsible for implementing operational resilience policy and reporting to the board. In any case, clear accountability and responsibility for operational resilience is required.

Companies will need to comply with requirements as soon as reasonably practical, with a hard stop of three years from the introduction of the rules (expected in the second half of 2020). At this point, firms are expected to have all elements in place, and be operating within their impact tolerances for their important business services.



3. Why is it happening now?

To remain competitive, companies are increasing innovation (including data driven innovation), digitisation and their use of the extended enterprise.

The increasing interconnectedness of the business world, as well as the increasing sophistication of threats, means that operational risk is now more dynamic, more complex, more important and more likely to crystallise.

People and organisations are increasingly dependent on financial services companies and their ability to deliver their services effectively.

There are significant numbers of services that both people and organisations don't want to perform themselves, where they recognise that others can carry them out more effectively. They want to trust their suppliers - and will increasingly only use companies they trust – to deal with stresses and disruptions, whilst delivering on their promises. This requires companies to be confident that their operational risk management can enable the outcome of operational resilience through both a change in mindset that joins the dots between different, existing capabilities and frameworks, as well as processes that adapt and evolve as the approach is developed, embedded, and enhanced.

4. The benefits of operational resilience

This change in mindset, and a positive approach to operational risk management and operational resilience, will help to:

- Enhance customer confidence and service
- Help firms react faster and more effectively
- Help make risk management more real
- Enable strategic foresight
- Enhance operational decision making
- Improve business performance
- Meet regulatory expectations

5. How companies can achieve the benefits of operational resilience

- Do understand your firm's current position
- Don't build a separate, siloed operational resilience framework
- Do evolve and iterate approaches
- Do use operational resilience to make operational risk management real
- Don't be restricted by the boundaries of your own organisation
- Do focus on internal collaboration between teams
- Do build in-house operational resilience capability and culture
- Do consider technology enhancement to drive efficiency
- Don't fail to engage the board, and particularly non-execs, early
- Do use operational resilience to support strategic decision making

Introduction

Operational resilience is now an imperative for regulated financial services companies in the UK. Increased innovation, digitisation, and reliance on the extended enterprise, coupled with recent high-profile technology-related incidents, have led to a collaborative supervisory initiative, intended to enhance operational resilience across the financial services sector. This paper has been written to help organisations extract value from the new regime, and to prevent it from becoming a compliance burden which yields limited business or customer benefits.

On 5 December 2019, UK regulators the Bank of England, the Financial Conduct Authority (FCA), and the Prudential Regulation Authority (PRA) published a shared policy summary and co-ordinated consultation papers on new requirements intended to strengthen operational resilience in the financial services sector. They want to ensure a stronger regulatory framework is in place to promote the operational resilience of firms and the financial market infrastructure.

Regulatory action on operational resilience began in June 2002, when the Bank of England launched the first of many market-wide exercises to assess and improve the financial sector's capacity to deal with major operational disruptions. Impetus for regulation has since been bolstered by concerns arising from widely reported incidents at regulated firms, and by the parliamentary prompting of the Treasury Committee, which has reviewed IT failures in the UK financial services sector.

Late in October 2019 the Committee published its unanimous finding that 'the current level and frequency of disruption and consumer harm is unacceptable' in the financial services sector. Subsequently, the regulatory triumvirate declared operational resilience to be 'no less important than financial resilience'. This is arguably a welcome re-balancing of focus; for too long, operational risk and resilience has been the 'poor relation' of financial risk and capital.

This paper is intended to help you digest the findings of the regulators' papers on operational resilience, to interpret what they mean for regulated companies, and to outline what steps must be taken. It will also show how the UK's new operational resilience regime will, if well implemented, deliver tangible business benefits and competitive advantage to companies in the financial services sector.

We hope you find this useful, and welcome your views on this topic.

Justin Elks
Managing Director
justin.elks@crowe.com

1. What is operational resilience?

Crowe defines operational resilience as:

The ability of a company to build confidence and trust in its capability to adapt to changing circumstances. This is achieved by preventing, responding to, and recovering and learning from stresses and disruptions whilst delivering on promises to customers, achieving critical business objectives, and operating within agreed tolerances.

The regulators' focus on operational resilience is 'top down', from the perspective of the resilience of the entire UK financial system. The importance of this is evident in the unusual tripartite cooperation of the regulatory bodies, which have worked together to build the operational resilience initiative. Perhaps understandably, the regulators' definition does not include the individual business benefits which should arise from well-implemented compliance efforts:

> Operational resilience [is] the ability of firms and Financial Markets Infrastructure (FMIs) and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions.

At Crowe, we see operational resilience as an outcome, rather than just a set of techniques. Like all effective risk management efforts, well-executed operational resilience approaches can and should deliver benefits beyond compliance.

Achieving these benefits, however, requires more than techniques. A change in mindset towards the management of operational risk and resilience is essential.

For UK and European re/insurers, operational risk is defined under the European Solvency II Directive as:

> The risk of a change in value caused by the fact that actual losses, incurred [due to] inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses.

The definition may appear narrow at first sight, but in practice encompasses almost any negative impact arising from the failure of people, processes, or systems, internal or external.

Operational resilience is the outcome of an effective operational risk management approach, one which connects the dots between functions and processes across an organisation.

2. Requirements of proposed UK regulation

The Bank of England, PRA and FCAs' shared policy summary and consultation papers, published in December 2019, build on concepts first set out in a joint Operational Resilience Discussion Paper published in 2018.

The publication sends a clear message that regulators will take a strong and consistent approach. They are seeking to ensure a resilient financial services system able to provide key services, with only limited interruption, when the system faces severe but plausible operational events. Key services include provision of the main mechanisms for paying for goods, services, and financial assets; intermediation between savers and borrowers, and to channel savings into investment via debt and equity instruments; and insuring against and dispersing risk. Regulators expect firms to extend their focus beyond the stability of their own firms to consider the impact of disruptions on other stakeholders, in particular the people and organisations that depend on them to deliver. If well executed, a firm will build trust, which will benefit their competitive position.

Regulation requirements

Under the proposed regulations, firms will need to:

- **Identify their important business services** that, if disrupted, could cause harm to consumers or market integrity, threaten the viability of firms and their safety and soundness or cause instability in the financial system.
- **Set impact tolerances for each important business service** which clearly quantify the maximum level of disruption they would tolerate, including time limits, within which they will be able to resume the delivery of important business services following severe but plausible disruptions. Dual regulated firms have the added complexity of developing impact tolerances that reflect the statutory objectives of the PRA and FCA.
- **Identify and map the chain of resources** that support their delivery of important business services.
- **Take actions to be able to remain within their impact tolerances** through a range of severe but plausible disruption scenarios. Firms should have contingency arrangements in place to enable them to resume the delivery of important business services.
- **Complete a regular self-assessment** to demonstrate compliance. This should be proportionate to the firm's activity, regularly updated and provided to the PRA on request.

The proposals aim to ensure that firms deliver improvements to their operational resilience in three main areas: Prioritising the things that matter; setting clear standards for operational resilience; and investing to build resilience.

Accountability and responsibility for operational resilience

Boards are expected to play a critical role in operational resilience as part of their responsibility to ensure a sound and well-run business. Ultimately, they need to take an active leadership role in ensuring that their company's operational resilience framework is fit for purpose, and that they have the management information, knowledge, experience and skills necessary to discharge those responsibilities.

Where it exists, the **Chief Operations role, Senior Management Function (SMF24),** is responsible for implementing operational resilience policy and reporting to the board. In any case, clear accountability and responsibility for operational resilience is required.

The board's responsibilities will include:

- Setting clear standards and satisfying themselves that the standards have been met.
- Ensuring that important business services have been prioritised and mapped effectively.
- Approving important business services and impact tolerances.
- Determining scenarios in which failing to remain within impact tolerances is acceptable.
- Overseeing and challenging senior management constructively.
- Approving and reviewing self-assessment reports, and satisfying themselves that the appropriate risk mitigation steps have been taken.
- Identifying critical dependencies on third parties and critical providers (including intra-group outsourcing).
- Making contingency arrangements.
- Promoting a culture of risk awareness and continuous improvement in operational resilience.
- Considering operational resilience when making strategic, operational and investment decisions.

Companies will need to comply with requirements as soon as reasonably practical, with a hard stop of three years from the introduction of the rules (expected in the second half of 2020). Whilst these timescales might not feel onerous, it is worth recognising that firms need at this point to be not only operating within their impact tolerances under normal circumstances, but also applying these principles and practices to their critical suppliers.

Third party requirements

Requirements related to outsourcing and third-party risk management are embedded within the FCA paper, but are the subject of a separate PRA consultation paper.

The draft supervisory statement in the PRA paper sets out more detailed guidance on how companies are expected to manage their third party risks, in the context of the greater adoption of cloud computing and other new technologies and the resultant changes to risk profiles.

Proposals include:

- Maintenance by all firms of their own Outsourcing Register, and submission of the information to the PRA, to enable the consideration of aggregate exposures and concentrations.
- The need to consider the proportionality of a firm or group and the materiality of the potential impact of outsourcing arrangements on the firm, including its operational resilience.
- Guidance on how to consider intra-group outsourcing proportionately, recognising it is not inherently less risky than external outsourcing.
- Boards take ultimate responsibility for the effective management of risk, identifying reliance on critical service providers and ensuring appropriate risk management systems are embedded.
- Detailed guidance on the contents of outsourcing policy.
- Minimum requirements for assessing materiality (including the provision of a definition and common criteria for material outsourcing), risk assessments, due diligence and for regulatory notification.
- Minimum contractual safeguards, including in respect of:
  - Data security
  - Access, audit and information rights
  - Sub-outsourcing.
- Requirements relating to business continuity plans, exit plans and strategies.
- Approaches to mitigating concentrations of risk.

The publication of these papers jointly, alongside references to the wider linkage to operational risk management and business continuity, shows the regulators are thinking holistically about firm resilience, including the extended enterprise and the wider risk management system.

The combination of enhanced requirements on third party risk and operational resilience could create challenges for firms with under-developed third party risk management programmes, in meeting the required timescales for implementing operational resilience.

3. Why is it happening now?

The changing face of operational risk

The risk environment, particularly for financial services organisations, has shifted in the past decade.

Many factors have contributed to this change, but technology and the use of third parties are both, and in combination, particularly important. Reliance on technology has increased in almost all processes, from front-end customer interaction to management, analytical, administrative, and settlement functions. Meanwhile the business world is increasingly interconnected. With a view to obtaining the benefits of increasing effectiveness, innovation, and cost efficiency, companies now often engage with external organisations to deliver and manage systems and processes which traditionally were undertaken in-house.

A related change is the greater ability of so-called 'bad actors' to disrupt businesses through systems interventions such as hacking. Similarly, the scope for human error by an employee or authorised insider or outsider to disrupt operations is possibly amplified by the penetration of technological processes. It was technology systems failures that prompted UK parliamentary interest in operational resilience.

Meanwhile, customer attitudes and trust toward companies are changing in this new environment. As people and organisations become increasingly dependent on financial services companies' ability to deliver services effectively, they want to trust the companies they use. We believe people and organisations will increasingly only use those companies which they trust to continue to deliver on their promises while dealing with stresses and disruptions.

Other trending factors are also important. Just-in-time delivery, globalisation, intellectual property breaches, multichannel sales, international sanctions, environmental awareness, and a host of other factors mean that operational risks have become:

- **More dynamic**
- **More complex**
- **More important**
- **More likely to crystallise.**

Addressing operational risks

Operational risks, which as we have seen may arise from the failure of people, processes, or systems, internal or external, may lead to disruptions which can be mitigated through operational resilience activity. Routinely navigating such risks effectively can lead to improved performance, which brings associated benefits to customers, shareholders, and other stakeholders.

Unfortunately, financial services organisations have frequently struggled to respond to operational risks with programmes of joined-up operational risk management that impact decision-making and support the delivery of strategic objectives.

Several factors have led to this shortfall including:

- Under-investment in non-financial risk approaches.
- Operational risk management approaches are typically bottom-up and granular, rather than top-down and holistic, and are only rarely linked directly to business strategy and decision-making.
- Disproportionate attention is often dedicated to risk assessment and to the cost and allocation of capital, to the detriment of focus on the use of these assessments to take action to prevent, respond to, and recover and learn from stresses and disruptions.
- Potential risks arising from new areas of corporate focus are often assessed in isolation, not as a part of enterprise-wide risk management activity, as illustrated by the use of siloed conduct risk frameworks in some organisations.

Lessons can be learned from the recent regulatory focus on conduct risk. Firms that built new frameworks which were not effectively integrated into their existing enterprise risk management and compliance frameworks incurred significant costs, created confusion within their businesses, and ultimately sacrificed the potential effectiveness of their approach to mitigating conduct risk.

As a consequence, operational risk management approaches within firms are not often seen as being effective, cost-efficient, or value-adding. If operational resilience is the outcome of effective operational risk management, these areas must be addressed as part of an effective operational resilience programme.

4. The benefits of operational resilience

A well-managed operational resilience approach can and should deliver extremely tangible benefits. Properly executed, operational resilience should yield not only greater resilience to shocks and disruptions, but also continuous improvements to customer outcomes, to create a genuine competitive advantage.

This is becoming clear to organisations outside financial services. For example, in October 2019 when reporting his company's quarterly results, easyJet Chief Executive Johan Lundgren referred directly to the airline's 'Operational Resilience programme, which has reduced [flight] cancellations by 46%, and lowered delays of thee hours or more by 24% year on year'.

So, to realise value from the UK's new operational resilience requirements, regulated financial services firms need to adopt a change in mindset that will drive a positive approach towards operational risk management.

This change in mindset needs to recognise that effective operational resilience cannot be achieved through an isolated function or framework driven by regulation and separated from other business functions or activity. Instead, it should be tackled by joining the dots between different, existing capabilities and frameworks, and through processes that adapt and evolve as the approach is developed, embedded, and enhanced.

The desired outcome is customer and wider-stakeholder confidence and trust in a firm's capability to deliver on its promises and achieve its objectives. To facilitate this, a clear link is required between business strategy and operational resilience. This requires not only that the delivery of operational resilience is embraced and given strong leadership at board level, but also that it is infused throughout the organisation, and permitted to cross the subtle boundaries that divide operational units.

Crowe has identified six broad categories into which the potential benefits will fall:

Enhanced customer confidence and service	The easyJet example above illustrates well the link between operational resilience and trust and confidence. If services are less likely to be disrupted, the downside risk of customer harm is reduced, and the upside benefit of enhanced trust increased. On a practical level, customers see that continuous, enhanced services will be maintained at times when less resilient competitors might lose traction.
Increased ability to react faster and more effectively	The likelihood and impact of lasting financial or reputational impacts arising from operational incidents and third-party disruptions is much reduced among companies which have implemented robust operational resilience programmes focused on fast recovery and learning lessons to enable continuous improvement.
Makes risk management more real	Operational resilience enhances the practicality and ownership of operational risk management across the enterprise by shifting the focus from the assessment to the management of risk. This creates a clearer link to business strategy and decision-making, and enhances the firm's organisational risk culture. This, in turn, drives operational risk awareness in the front line.
Enhanced strategic foresight	People often underestimate uncertainty. Operational resilience delivers insights into the effectiveness of operational delivery by learning lessons before new events impact operations.
Enhanced operational decision making	Operational resilience can deliver insights into how operational delivery and a company's business model support the realisation of business strategy. This in turn can enable firms to increase the efficiency and effectiveness of their business models, and enhance decisions to balance value, cost, risk, and resilience. By doing this, companies will meet regulatory expectations as a by-product. In contrast, a purely regulatory-driven approach will limit these benefits.
Improved business performance	By joining the dots between existing, siloed operational functional areas of the organisation, operational resilience delivers a cost-efficient evolution of the interrelationships between business units, thereby improving operational outcomes overall. This will help to maximise the return on investment for resilience frameworks.

5. How firms can achieve the benefits of operational resilience

Ten golden rules for creating value through operational resilience

The following ten golden rules will help to ensure that any newly established operational resilience approach will yield strategic value.

✔ **Do understand your firm's current position**
Firms should understand how the elements of resilience are currently working before rushing to mobilise a large, costly programme. Conduct an independent-minded gap analysis across enterprise-wide existing capabilities and resources, to ensure you focus and prioritise the right activities.

✘ **Don't build a separate, siloed operational resilience framework**
Instead, join the dots between existing capabilities and approaches by building on established operational components that contribute to resilience.

✔ **Do evolve and iterate approaches**
Effective development will be evolutionary, not revolutionary. Refine tools and techniques in an iterative process which helps to build enterprise-wide understanding of and engagement in operational risk and its mitigation.

✔ **Do use operational resilience to make operational risk management real**
An operational resilience approach can reach its full potential only when enhanced action, risk-based decision-making, and proactive business behaviours come into focus. Use your operational resilience work to shift your firm's risk focus from identification and assessment to operational risk management. That will make the process more engaging for everyone in the business.

✘ **Don't be restricted by the boundaries of your own organisation**
The actions of third and even fourth parties often have an enormous impact on an organisation's operational resilience. Ensure that the focus of third party risk management reflects your own business model properly and robustly, and therefore addresses the risks where and when they arise.

✔ **Do focus on internal collaboration between teams**
Whilst someone must 'own' and be accountable for operational resilience, almost all business areas must contribute. It is important that boards, executive management and senior management are engaged from the beginning and consulted throughout the programme to ensure a shared sense of ownership across the firm.

✔ **Do build in-house operational resilience capability and culture**
With resource often in short supply, companies may outsource the operational resilience challenge to a third party in order to build momentum. Whilst beneficial in the short term, this approach is unlikely to create a sustainable programme or add real value. Instead, work collaboratively with partners who prefer to cooperate with you, rather than simply do a project to you in order to build your in-house capabilities through the engagement of individuals in practical, relevant activities.

✔ **Do consider technology enhancement to drive efficiency**
Understanding operational resilience requires the ability to integrate and synthesise information and perspectives across business silos. Reviewing and enhancing technology to meet resilience requirements will help to ensure operational resilience compliance and implementation does not become manually intensive and cost inefficient.

✘ **Don't fail to engage the board, and particularly non-execs, early**
Frequent and robust discussion of operational resilience issues will garner the attention and interest of individual directors. Present discussion points early to facilitate board-level focus on important risk factors which have become more important, more dynamic, and more likely to crystallise, but otherwise may be overlooked. Doing so will prompt your board's earlier, strategic engagement in critical business decisions.

✔ **Do use operational resilience to support strategic decision making**
Executed well, operational resilience can bring valuable insights into the ways in which processes and business models contribute to (or detract from) the achievement of business strategy, and illuminate potential changes that would optimise them, improve performance, and build resilience. Approach operational resilience in this way so that it is transformed from a compliance project focused on downside risk into a tool to improve your firm's ability to identify, manage, and profit from opportunities.

6. How Crowe can help

Crowe adopts a collaborative approach to operational resilience. Our work aims to help clients develop the internal capabilities to enhance operational resilience, and to realise the many tangible business benefits that a robust, well-managed, joined-up approach will yield.

Resilience Approach Assessment & Development

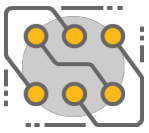
Operational Resilience Strategy

Important Service Mapping & Optimisation

Integrating Resilience into ERM

Incident Planning & Management

Capability & Culture Development



Technology

Reporting & MI

Testing & Assurance

Governance & Accountability

About Us

Crowe is a global professional services company working across the areas of consulting, audit and tax with our UK consulting practice specialising in financial services. We combine deep risk management and governance expertise with innovative thinking to solve clients' challenges. Our collaborative and progressive approach allows us to create lasting value for our clients and is focused on four key areas: mastering data, building resilience, delivering transformation and enhancing strategy.

Contact Us

Justin Elks, Managing Director
justin.elks@crowe.com

Daniel Bruce, Partner
daniel.bruce@crowe.com

crowe.com/uk-consulting