IMPACT STUDY | In association with: BMC

FIVE FACTORS TO CONSIDER WHEN BUILDING OPERATIONAL RESILIENCE

OCTOBER 2021

Finextra | bmc

Contents

01 | Introduction

The term resilience is receiving a significant amount of airtime in 2021. While the pandemic certainly pulled into focus the need for resilient systems across financial services, the push toward financial resilience was first born in response to the 2008 financial crisis.

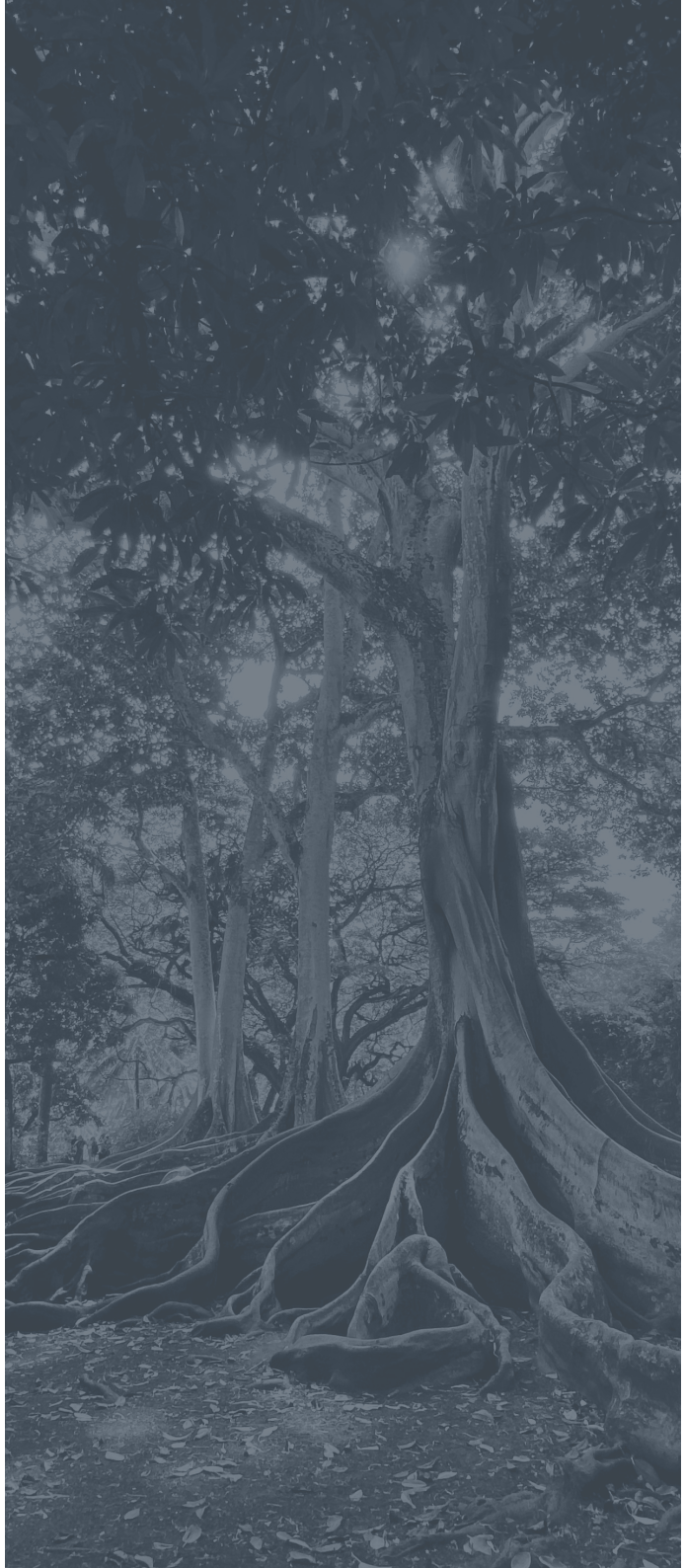
Since 2008, focus has shifted toward building resilience across operations in the financial services sector, by assessing vital business functions, setting levels of tolerance that these functions can withstand, and testing the tolerances at regular intervals.

The Basel Committee on Banking Supervision **defines** operational resilience as the ability of a bank to deliver critical operations through disruption. This ability enables a bank to:

- Identify and protect itself from threats and potential failures;
- Respond and adapt to – as well as recover and learn from – disruptive events.

Unlike typical risk management or more traditional compliance-based approaches, when it comes to operational resilience, banks should assume that disruptions will occur – and consider their overall risk appetite and tolerance for disruption. In the context of operational resilience, the Committee defines tolerance for disruption as the level of disruption from any type of operational risk a bank is willing to accept, given a range of severe but plausible scenarios.

According to the businesses **McKinsey** works alongside, resilience isn't just about dealing with the issues and challenges of today. It's also about creating a culture fortified with technology and digital tools that enable them to be ready for impending changes: "The very definition of resilience—the ability to recover quickly from difficulties—is being deployed across these companies with striking speed.



Now is not the time to hit pause. Now is the time to reimagine supply chains, adapt and overcome the longstanding idea that there needs to be a trade-off between efficiency, growth, and resilience."

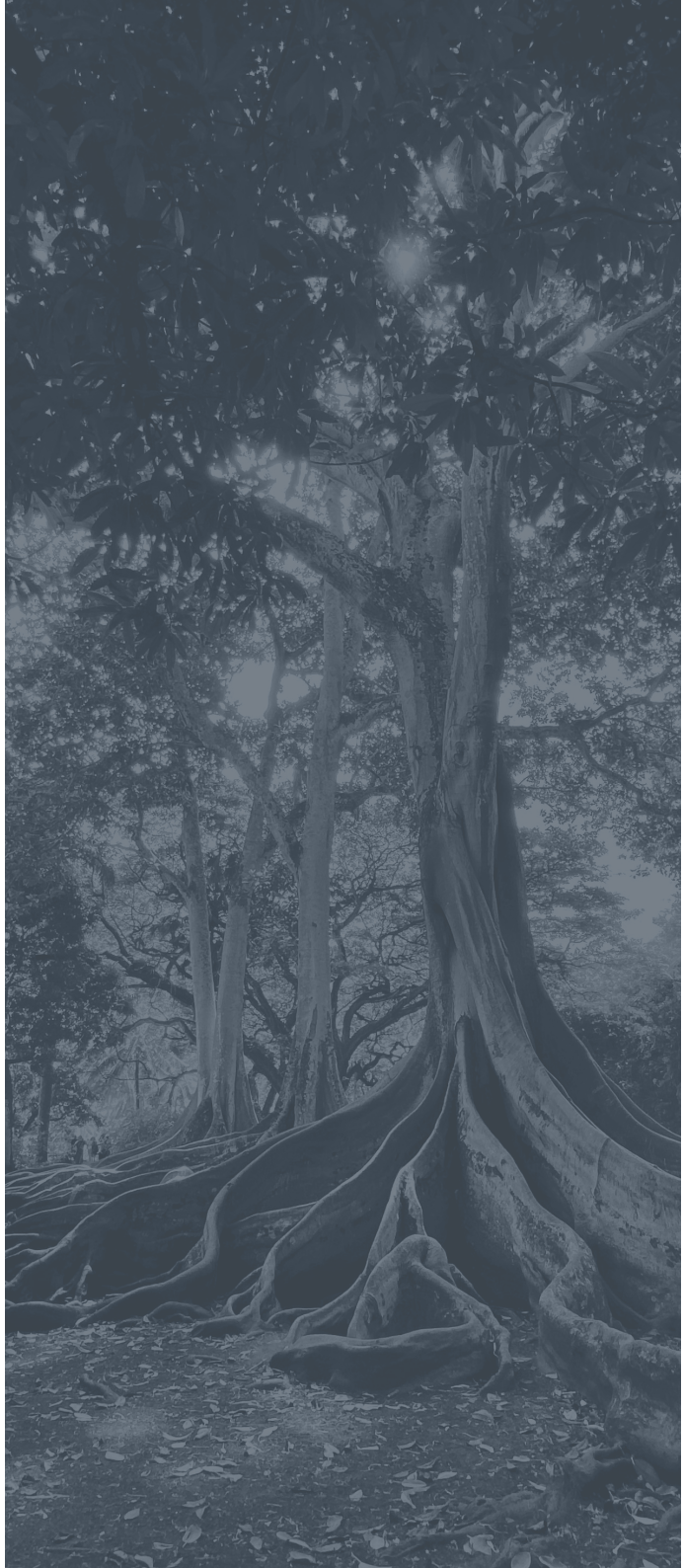
Operational resilience is defined in quite broad terms within most schemes across the globe. The US, EU, Hong Kong, Singapore, Australia, and the UK are all working toward similar objectives, with their strategies informed by existing regulatory guidance around risk management and governance, as well as output developed by global standard bodies, such as the Basel Committee and the Financial Stability Board.

UK regulators, for instance – including the Bank of England, Prudential Regulation Authority, and the Financial Conduct Authority – have prioritised operational resilience over the past three years.

Unavailability of vital business services and operational disruption have the potential to cause significant harm to consumers – in turn, posing a risk to market integrity, threatening the viability of firms, and causing instability across the financial system. The Financial Conduct Authority (FCA) **observes** that disruptions caused by the coronavirus (Covid-19) pandemic reveal why it is vital for firms to understand the services they provide, and invest in their resilience.

In March 2021, UK regulators published a final **policy summary** on operational resilience expectations, mandating that by the end of March 2022, firms and financial market infrastructures must:

1. Identify their important business services by considering how disruption to the business service they provide can have impacts beyond their own commercial interests;
2. Set a tolerance for disruption for each important business service; and
3. Ensure they can continue to deliver their important business services – and are able to remain within their impact tolerances – during severe (or in the case of FMIs, extreme) but plausible scenarios.



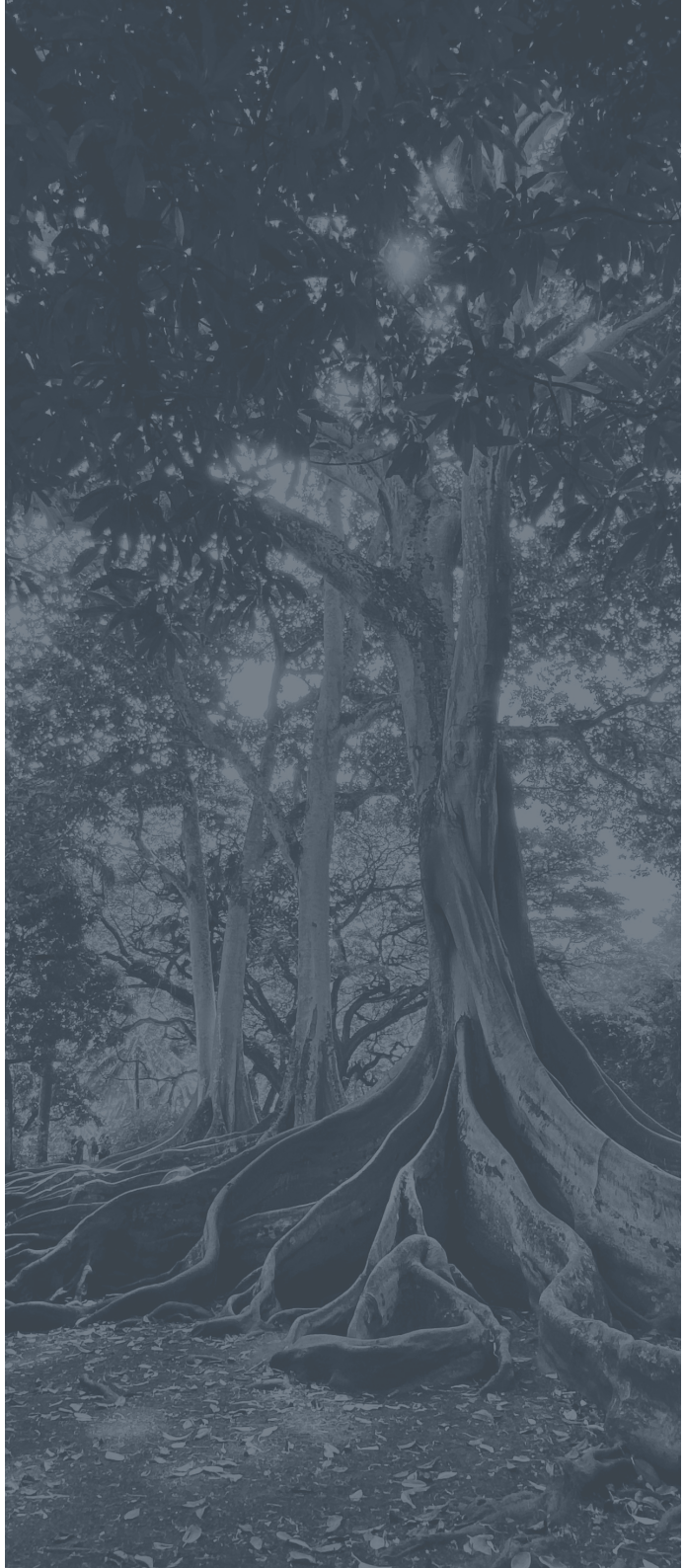
Even at first glance, these expectations present a monumental challenge for incumbent financial institutions, which – given both the Covid-19-induced business pressures and cut-throat competition from nimble digital players – already find themselves in unfamiliar waters.

What's more, within these already tight deadlines, authorities expect banks' operational resilience to become a repeatable and dynamic activity. Indeed, firms' impact tolerance and the resilience plans they implement, to stay within those tolerances must be continually updated in order to take into account any circumstance changes.

Prior to such requirements being set in stone in the UK or across the globe, the consultation period saw many firms ask the regulator to spell out precisely what is expected of them in practical terms. Recognising that financial institutions have fundamental differences in their infrastructure, and are each at different stages of their resilience testing process, regulators refused to enumerate specific guidance in how firms should approach this task.

This has left firms with the complex challenge of meeting regulatory outcomes without explicit guidance or steps on how to achieve them. Yet, with the correct tools and a technology-centric mindset, institutions can tackle these regulatory demands with a suitable technology partner, strengthen their core systems, and position themselves to achieve compliance in a shorter timeframe.

While the ability to predict which areas are likely to cause disruptions was once the purview of a human supervisor, given the shift to digital operations, it is only logical that firms employ tools such as artificial intelligence (AI) and machine learning (ML) to identify patterns and risks within an institutions' complex technology systems. This impact study outlines five key considerations that financial institutions must be aware of, ahead of impending regulatory deadlines, as well as the technology-based solutions available to assist them in building a robust and compliant operational resilience strategy.



02 | The first hurdle: grappling with identification and mapping

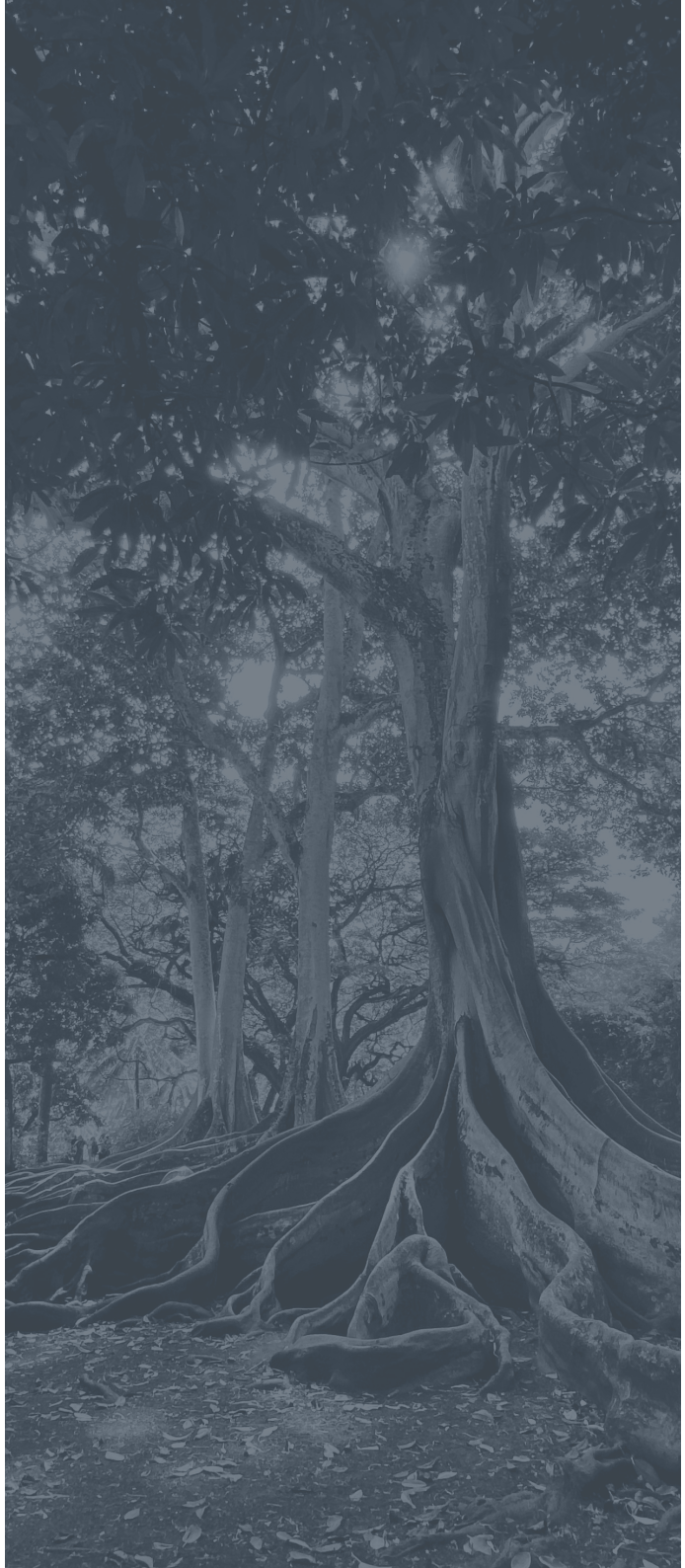
Identifying and mapping the key technology which supports important business services is a key obstacle firms must grapple with.

Risk identification is a fundamental component of effective operational risk management systems and is particularly challenging for large financial institutions that are juggling, on one side, the pressure to innovate and evolve digitally, and on the other, the need to comply with sweeping regulatory updates. Many of these updates are themselves aimed at attempting to supervise the new and highly digital future of financial services.

In its **Consultative Document**, 'Revisions to the principles for the sound management of operational risk,' the Basel Committee lists a selection of tools which are useful for identifying operational risk.

These tools include:

- Operational risk event data;
- Self-assessments;
- Event management;
- Control monitoring and assurance framework;
- Metrics;
- Scenario analysis; and
- Benchmarking and comparative analysis.



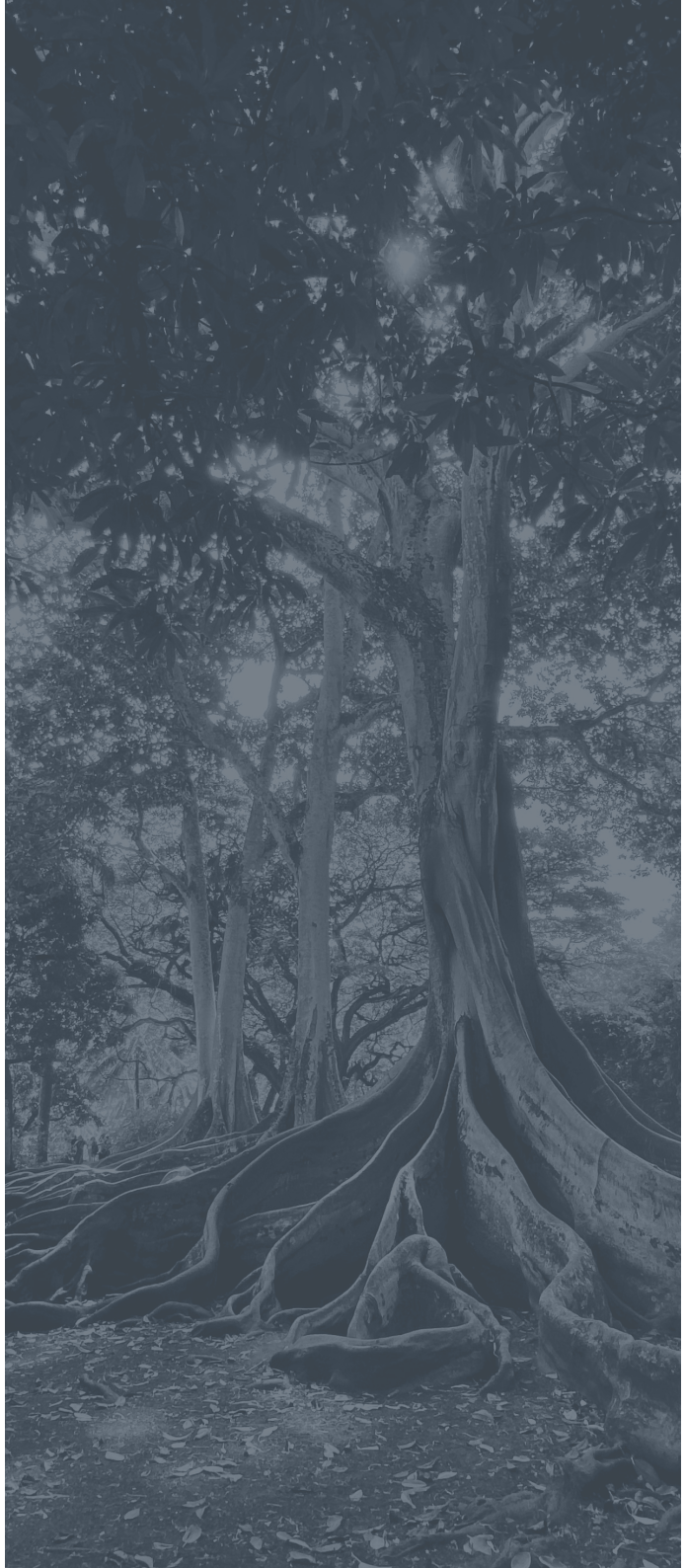
To accurately identify risks, the output of these tools must be based on accurate data. The integrity of this data is ensured by strong governance and robust verification and validation procedures, and adequately takes into account the internal pricing and performance measurement mechanisms as well as for business opportunities assessments.

Once a financial institution has identified its critical operations, the next step is to map the internal and external interconnections and interdependencies that are necessary for their delivery. This involves the identification and documentation of the people, technology, processes, information, and facilities involved, including those which may be dependent upon third parties.

Indeed, when it comes to operational resilience, this interconnectedness of financial services creates something of a double-edged sword. Interdependencies throughout the ecosystem are complex, which is reflected in the web of services large financial institutions provide within their own offering. It is therefore considerably challenging to unravel and precisely identify specific business services that are often entwined across multiple offerings, platforms or systems within a given institution.

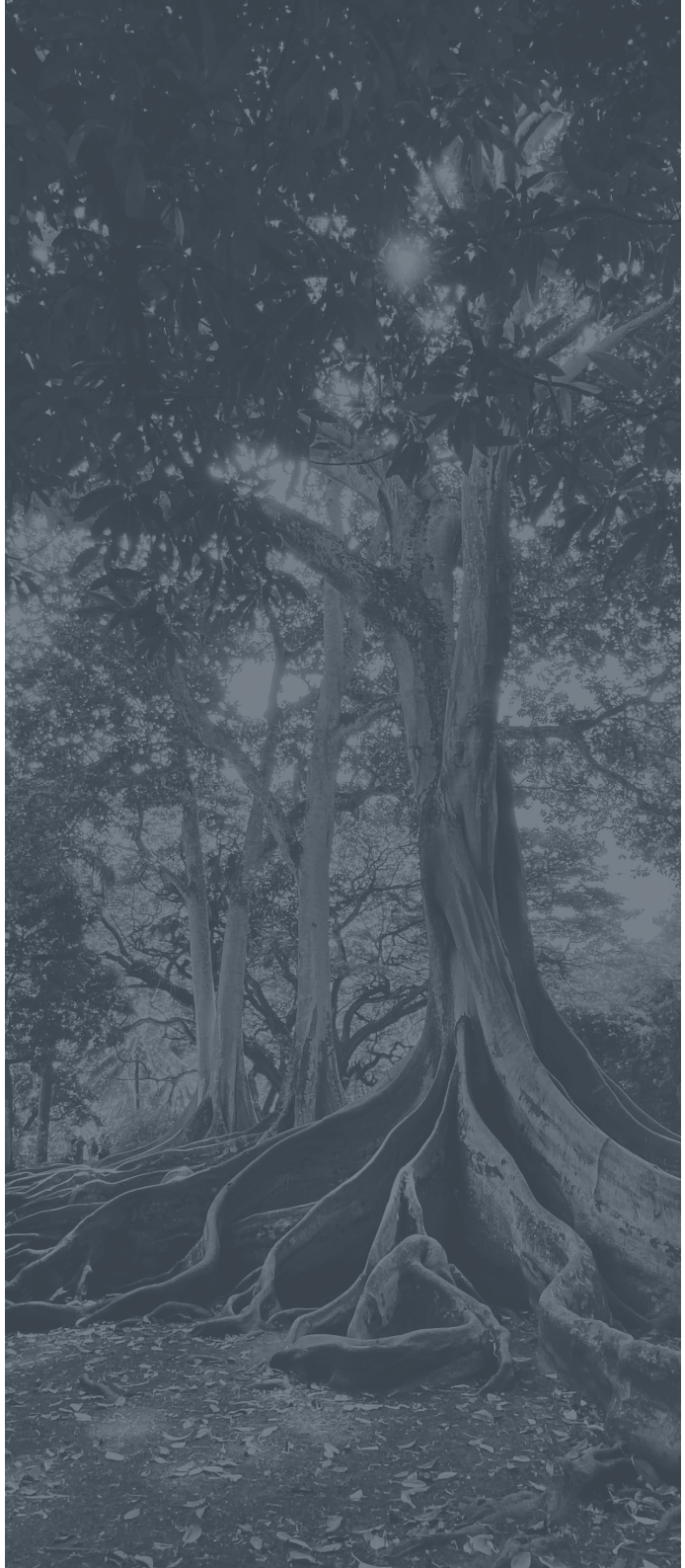
Outsourcing arrangements that may have been less complex in the past – when systems were more commonly tied to 'brick and mortar' business functions – are now obliged to protect against new risks and digital threats that may emerge through projects such as cloud migration or third party-licenced software as a service (SaaS).

Through the lens of Covid-19 impact, **McKinsey** explains that while digitisation efforts can present a complicated risk-profile for banks, accelerating these plans can also enhance safety efforts toward reduced contact by enabling omnichannel interactions. For instance, when consumer banks accelerate the consolidation of physical-branch networks to reallocate resources and serve customers more effectively through digital channels, this has the effect of reducing in-person contact and potential exposure—but also reduces the bank's opportunity to connect with customers on a human level.



Varying priorities, culture, investment cost and complexity are common roadblocks in the push for operational resilience, and serves to highlight the need for cultural changes to be implemented when working toward operational resilience. Given the interconnectedness of financial services, it has become commonplace for a single business service to extend across multiple technologies and third parties. When location, potential for cyber-crime, and human-based risks culminate, the gathering of relevant data points for mapping and reporting becomes highly challenging.

Defining ownership boundaries is essential in assisting firms to measure, manage and drive resilience for the critical cross-team business services that are identified. Further, Accenture **notes** that relevant teams should provide input into the assessments, improving and testing their component of the service.



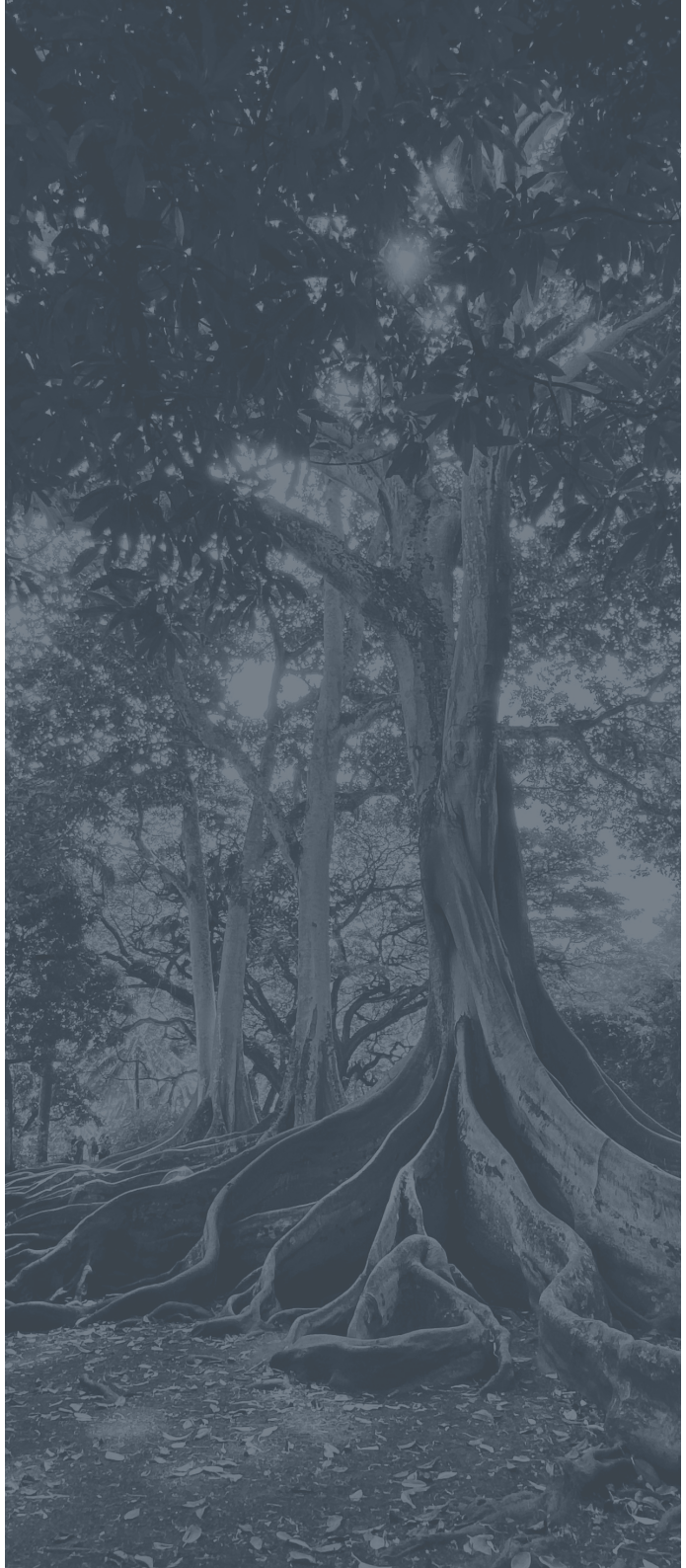
03 | Testing on the go: assessing and testing business service tolerance

As mentioned previously, a fundamental element in the development of strong operational resilience is the assessment and testing of impact tolerances. Once firms have laid out their tolerance levels – typically the maximum tolerable level of disruption to an important business service – they should be tested against dynamic scenarios to ensure that they can be met.

Indeed, a recurring requirement in operational resilience guidance across the globe is the need for repeatability. For example, without mandating a specific number or volume of testing, the Bank of England (BoE) and the FCA have outlined that while testing should not become "unduly burdensome," the process of testing regularly and reviewing mapping processes at least annually is required for firms to "better understand their systems and identify any vulnerabilities that need remediation."

With the outcomes of scenario testing expected to be regularly logged and updated, it is prudent for firms to consider utilising tools and services that not only assist with executing (at a minimum) annual testing, but also streamline and strengthen the metrics used as parameters within the testing itself. Technology that delivers accurate business forecasting, clear cloud migration simulations, robust assessment of risk and vulnerabilities, or the reliable breakdown of future updates and releases, is highly valuable when attempting to generate consistent and precise inputs for scenario testing.

Given the obligation to report the methodologies employed to generate metrics and undertake scenario testing, leaning on the technological capabilities of specialised providers is a shrewd strategy for financial institutions. This point is raised by the Basel Committee, which notes that the approach and level of granularity of mapping should be sufficient for banks to identify vulnerabilities, as well as to test their ability to deliver critical operations through disruption – while factoring in the bank's risk appetite and tolerance for disruption.



04 | Getting back on track: understanding response and recovery for system failures

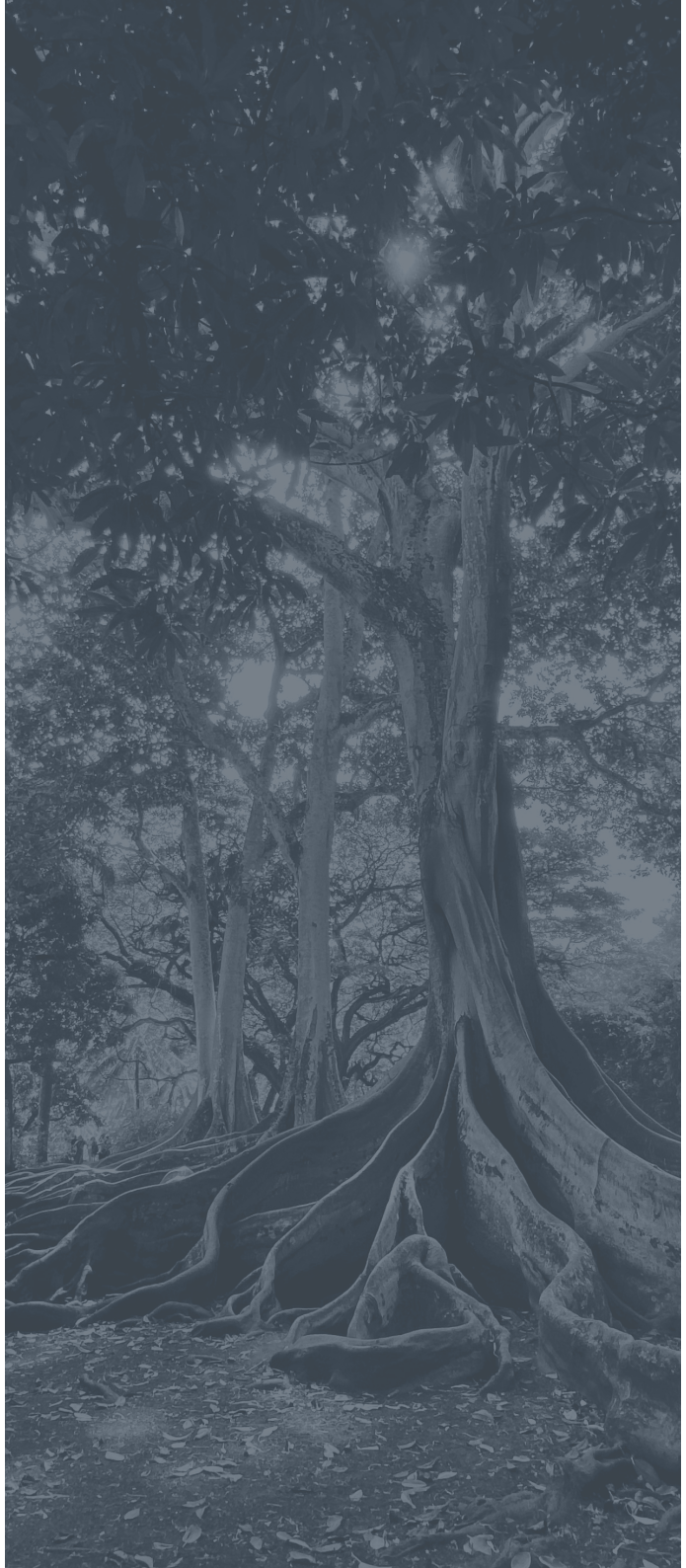
Maintaining and improving enterprise resilience is also a means for organisations to build trust not only with their customers, but with regulators and the underlying economy. System failures are problematic not only for short-term system outage and accessibility reasons, but damage the reputation and trust financial institutions have spent decades building, in the long-term.

An example of the need to perfect a clear strategy around operational resilience can be seen in the collapse of the European Central Bank (ECB)'s Target2 system during 2020, which left commercial banks unable to service their customers for 11 hours. No electronic Euro payments across Target2, TIPS, SEPA and EURO1/STEP1 were able to be settled during the outage, which the ECB states was the result of a software defect in a third-party network device.

This major incident was a wakeup call not only to payment infrastructure providers, but to hundreds of financial institutions that rely on them to deliver core business functions. Setting aside the regulatory obligation to develop a robust operational resilience strategy, financial institutions can no longer ignore the need to plan for such events, if they wish to remain competitive.

Delivering a reliable service is critical. Having alternative strategies in the event of a system failure secures customers' trust. Leveraging multi-cloud service management arrangements, for instance, can help protect a financial institution's critical business offering and data, by providing backup and recovery capabilities for business continuity.

Enhancing AIOps strategy is another approach that can strengthen an institution's operational resilience. By combining big data and ML to automate IT operations processes – such as anomaly detection, event correlation and causality determination – AIOps can help detect and predict complex failure conditions within huge data sets and intricate systems.



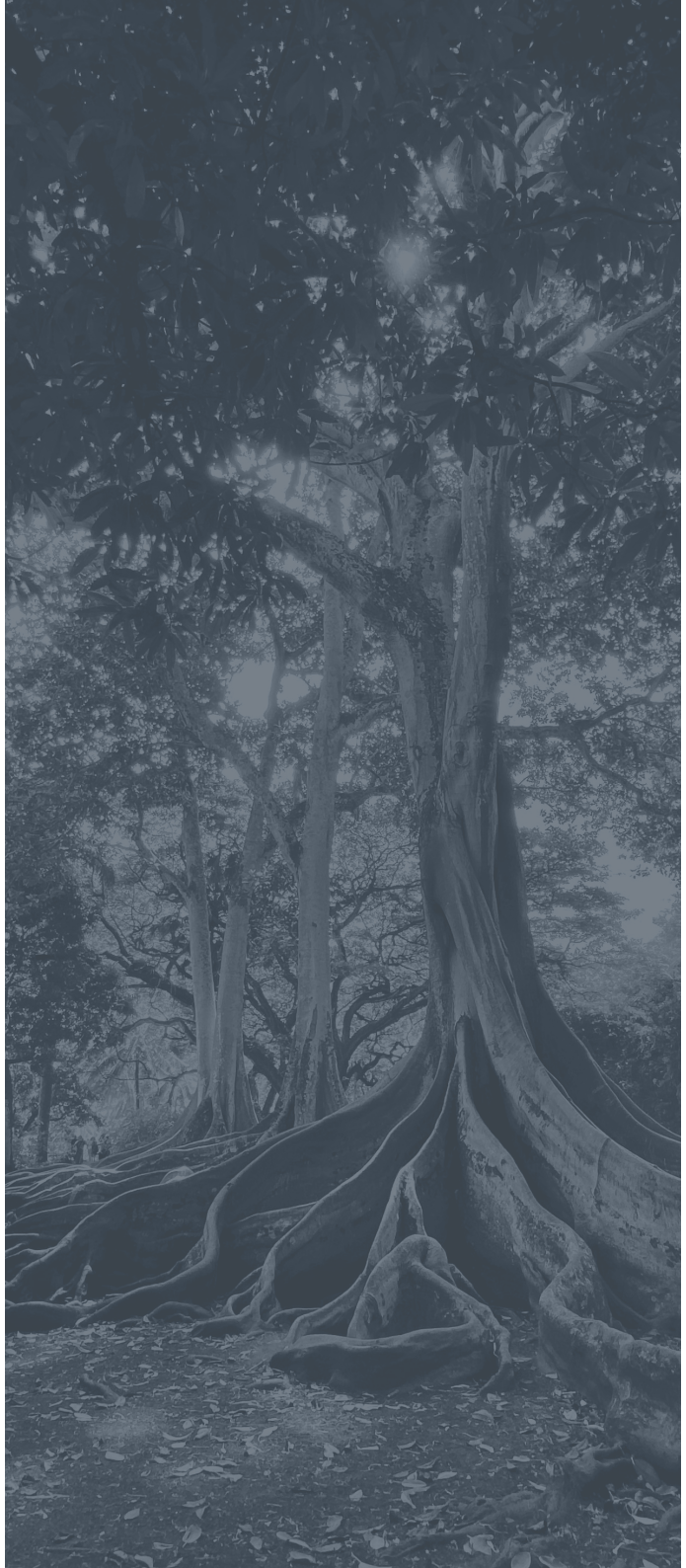
05 | Reducing vulnerabilities: strengthening security and governance to combat cyber threat

As a result of widespread digitisation, financial services are more interconnected and reliant on third parties than ever before. This connectedness, while providing fertile ground for innovation and collaboration, means that the ecosystem is highly vulnerable to security threats and attacks. Should bad actors succeed in targeting a specific player within the system, it is likely that any outage or failure would impact multiple institutions, and in turn, many customers.

In addition, cyber-attacks are typically difficult to identify, and the breadth of these attacks can be a slow and painstaking process.

Given the scale and speed at which cyber-attacks can threaten the security of a financial institution, firms should look to technology that is specifically crafted to improve systemic resilience. Tools like vulnerability management – which continuously scan systems to identify, prioritise, remediate, and report on security vulnerabilities – can be invaluable; particularly when combined with robust patch management regimes.

The intricacy of regulations that govern the financial services landscape are increasingly challenging to traverse, and financial institutions that fall short of their compliance obligations run the risk of incurring significant financial penalties. Tools that continuously audit internal compliance regimes can offer a level of operational resilience that is in line with stringent regulatory frameworks and are therefore critical for firms looking to ensure they are protected against new and sophisticated threats.



06 | Communicating the value of business metrics and streamlining workflows

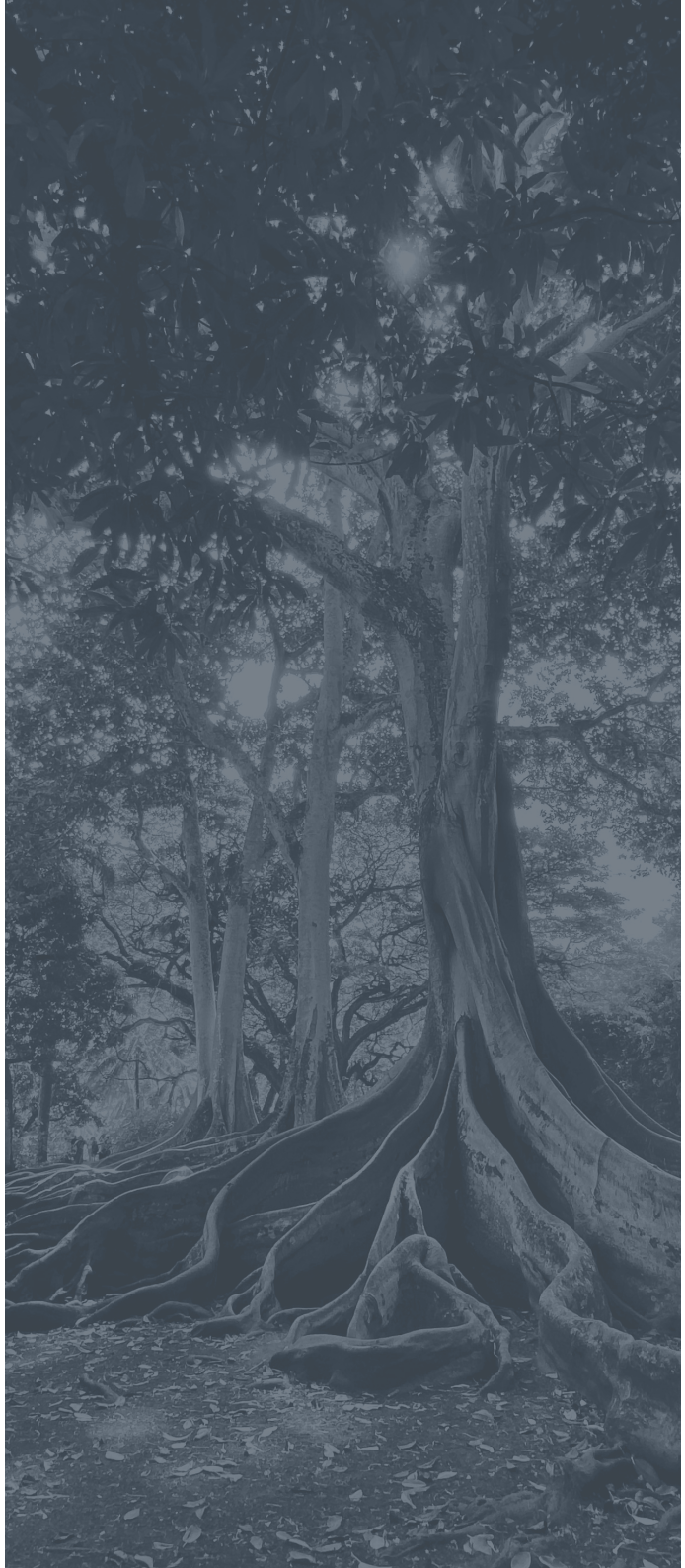
Communications play an integral part of overarching operational resilience capabilities and are therefore held to the same governance requirements. Given this increased obligation, it is vital for financial institutions to provide adequate training to their communications and operations functions.

Deloitte **explains** that such training will lead to the establishment of defined and rehearsed communications plans and procedures, including full consideration of any necessary surge capacity alongside stakeholder mapping, and an understanding of vulnerable stakeholders relevant to the business services affected.

"These should be tailored to specific scenarios and cover key aspects such as pre considered actions for customer redress. The operational resilience approach will need to involve communications specialists and confirm the message and suitability of communications channels," notes Deloitte.

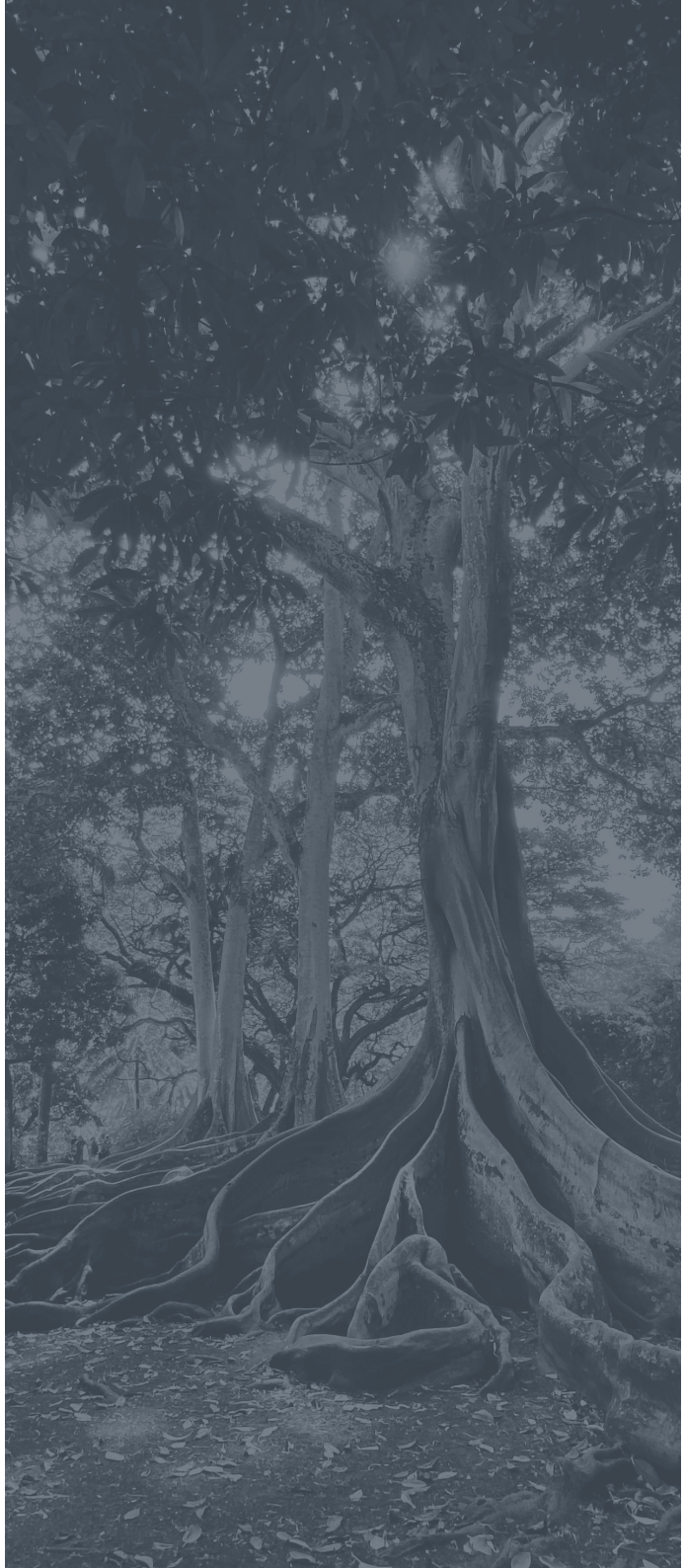
Naturally, visibility and communication are intrinsically tied to the pursuit and development of operational resilience. However, since technology teams within financial institutions have historically operated in silos, streamlined sharing of information is not commonplace – making it difficult to achieve a holistic view of technology assets and the services that this technology should support.

This challenge is increasingly being addressed through the adoption of tools which work to improve visibility across a business's entire ecosystem. A single dashboard can offer an automated platform where information is collated and presented in a systematic and consistent manner – streamlining assets and relationships into a single view, and building a more thorough, resilient source of information.



Intelligent, automated workflows present another attractive means for financial institutions to bolster business adjacencies and build on their operational resilience. Put simply, a lack of IT workflow integration and co-ordination leads to inefficiencies, lost productivity, and security weaknesses, which jeopardises resilience-building efforts.

Technology targeted at injecting AI-powered analytics and ML tools serves to rectify disjointed, manual and inaccurate processes and communications, and helps to drive better decision making via the delivery of accurate and complete data. Also, automation can pre-emptively offer application delivery, deployment and configuration, which each contribute to the development of a robust operational resilience regime.



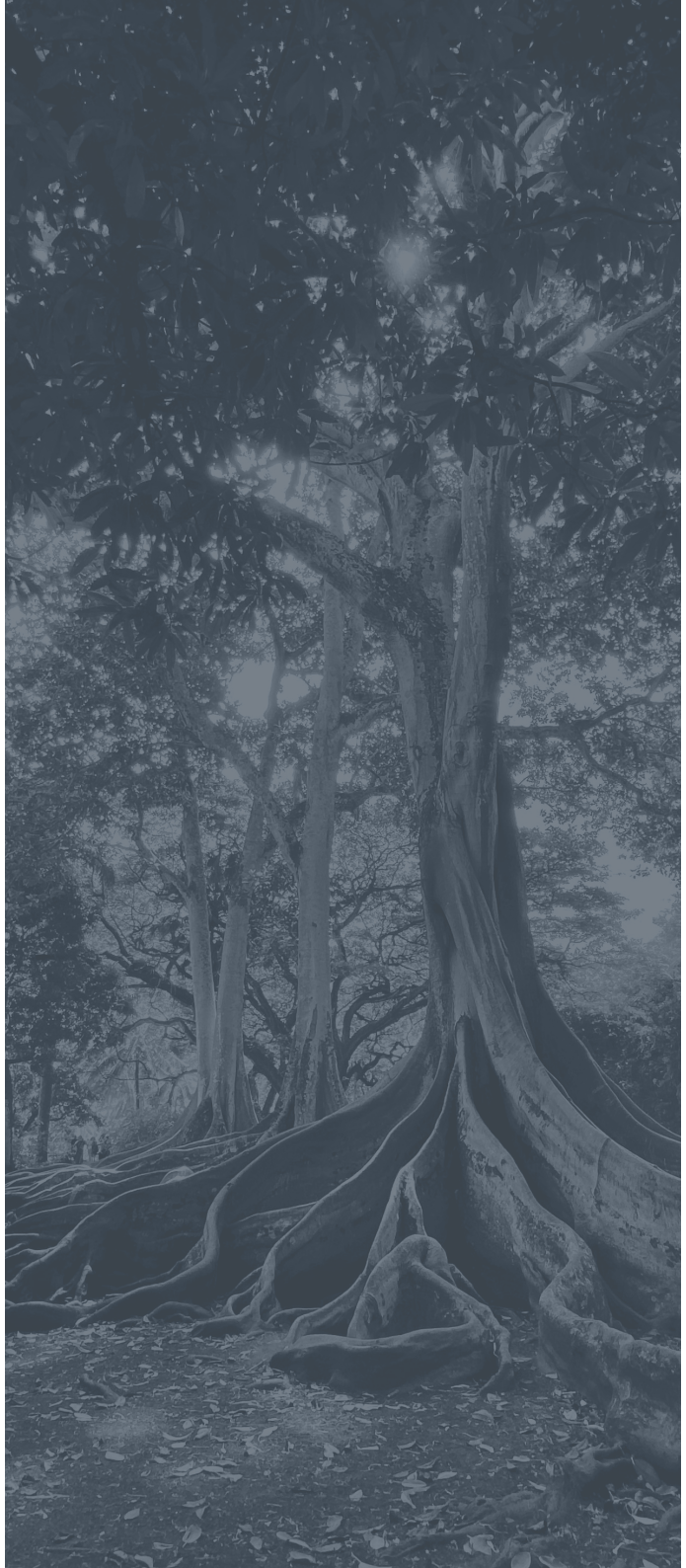
07 | Conclusion

Operational resilience is only moving up the regulatory agenda across the globe. While slight variations in requirements exist from jurisdiction to jurisdiction, what remains consistent is both the breadth and the importance of developing and maintaining a robust operational resilience strategy.

While it is useful for firms to first build a clear understanding and strategy around how to interpret and apply regulatory guidance, identifying the tools and services that can assist in the effective delivery of these objectives is pivotal.

Given the operational resilience mandate emerged in (significant) part as a response to the increasingly digital, interconnectedness of the financial services sector, it is only logical that firms look to technology – which has been specifically designed to assist in its management – for support; rather than clinging to traditional compliance approaches.

Technology service providers that are well equipped to support financial institutions in their quest toward building operational resilience are those with a keen awareness of the need to develop alongside both the financial institutions they serve, and the evolving regulatory landscape in which they operate.



About

Finextra Research

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology (FinTech) news and information source.

It offers more than 100,000 FinTech news, features and TV content items to visitors to **www.finextra.com**.

Founded in 1999, the business covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organizations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 FinTech professionals working inside banks and financial institutions, specialist FinTech application and service providers, consulting organizations and mainstream technology providers. The Finextra community actively participates in posting opinions and comments on the evolution of FinTech. In addition, it contributes information and data to Finextra surveys and reports.

For more information:
Visit **www.finextra.com,** follow **@finextra,** contact **contact@finextra.com** or call **+44 (0)20 3100 3670.**

BMC

From core to cloud to edge, BMC continues to build on a 40-year heritage of shaping digital transformation for organisations around the world. We deliver the software and services innovations that help over 10,000 global customers, including 84% of the Forbes Global 100, thrive in their ongoing evolution to an Autonomous Digital Enterprise — where manual effort is minimised to capitalize on human creativity, skills, and intellect across the enterprise, and businesses learn to continuously examine customer and partner relationships to intelligently create new value.

Our future-focused portfolio helps drive business success with AI-enabled solutions for service management, automation, optimisation, performance, and security, covering everything from mainframe to multi-cloud. BMC's open, scalable, modular technologies help ensure that our customers can run and reinvent their businesses for growth and competitive edge while optimising cost, performance, and security.

For more information

FINEXTRA RESEARCH

77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Follow
@finextra

Web
www.finextra.com

Finextra | bmc