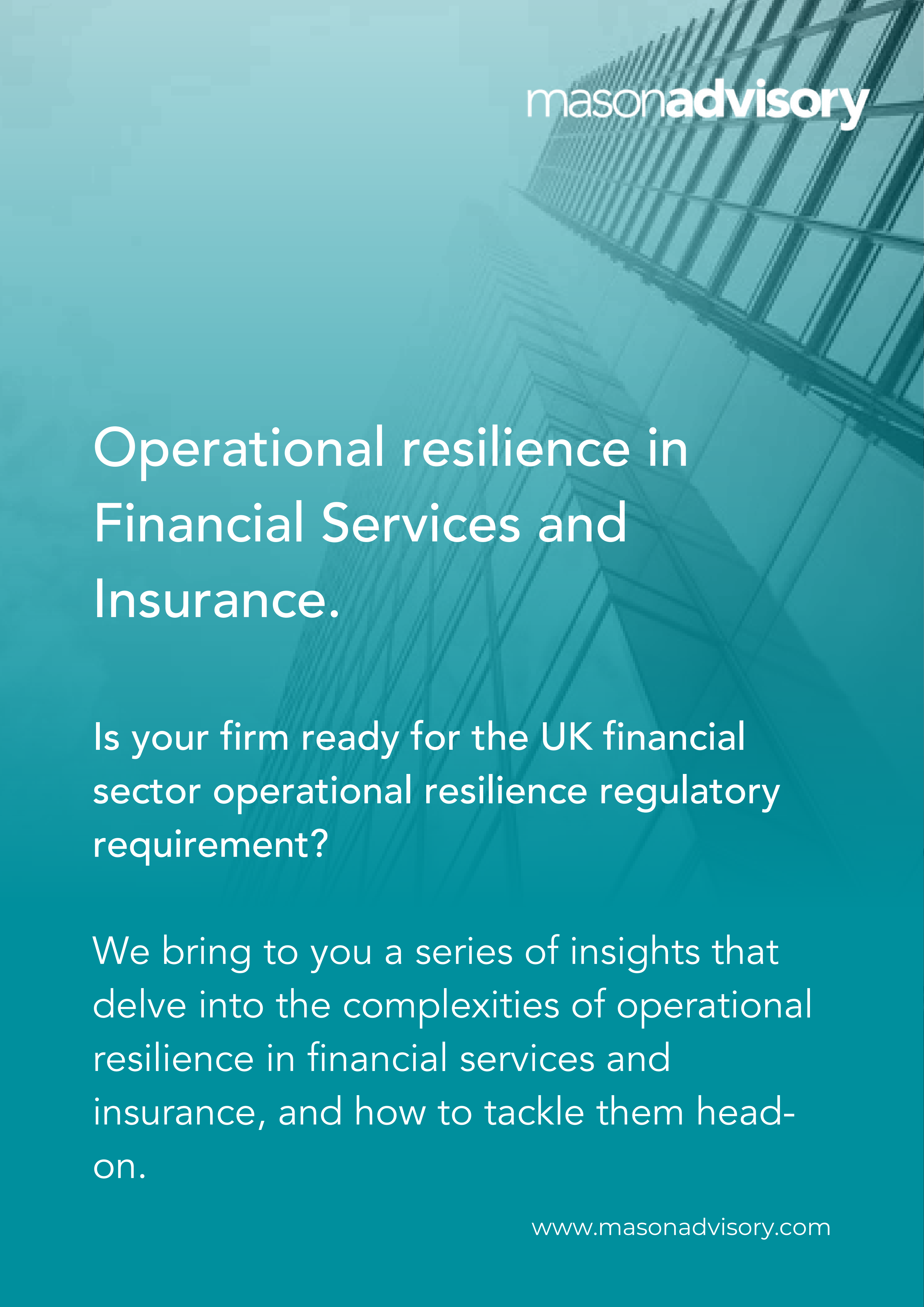


masonadvisory

Operational resilience in Financial Services and Insurance.

Is your firm ready for the UK financial sector operational resilience regulatory requirement?

We bring to you a series of insights that delve into the complexities of operational resilience in financial services and insurance, and how to tackle them head-on.

www.masonadvisory.com

Content

INTRODUCTION

Financial services operate within intricate systems involving numerous interconnected entities, processes, and technologies. Disruptions in one area can quickly propagate across the entire ecosystem, leading to widespread consequences. Being prepared ensures that institutions can effectively manage and mitigate such cascading effects. But identifying the key priorities, how to address them, and in what sequence, can be a real challenge.

At Mason Advisory, we understand the critical importance of operational resilience in the ever-evolving landscape of financial services. That's why we're excited to introduce our comprehensive Operational Resilience Framework for you to download. It is designed to align with Prudential Regulation Authority (PRA), FCA (Financial Conduct Authority) and DORA (Digital Operational Resilience Act). requirements, principles, and guidelines. But it also provides the practical foundations from which to integrate true resilience across your whole organisational ecosystem.

This series of insights explore the complexities of operational resilience and how to tackle then head-on.

Insight overview

Insight 1 of 3 - The right resilience roadmap starts with the right questions

Operational resilience in financial services, why this should be an enterprise-wide concern, not simply IT’s remit. Mason Advisory Managing Director, Jon De’Ath, takes a look at the tricky area of operational resilience in financial services and explains why this should be an enterprise-wide concern, not simply IT’s remit.

For financial services organisations, there's a perfect storm looming. Updated regulatory requirements, published by the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA, Bank of England), are coming into force, fast. The first policy milestone is now firmly in the rear-view mirror, having passed in March 2022. Firms now only have until 31st March 2025 to comply fully with the new requirements and operate within their impact tolerances.

Even in isolation, aligning to this updated regulatory landscape would be a complex undertaking. But the story doesn't stop there. At the back end of 2022, the Council of the EU officially adopted the Digital Operational Resilience Act (DORA), designed to ensure that the finance and insurance industries in Europe are equipped to stay resilient through severe operational disruption. Although the legislation does not directly apply to the UK, any organisation seeking engagement with, or already engaged with, a European company, will most likely need to comply. That time scale is even more pressing, with a deadline for compliance of the 25 January 2025.

Together, these scenarios represent quite a headline on any technology leader's worry list! But, when set against a backdrop of global volatility (the pandemic, BREXIT, the war on Ukraine, unstable supply chains, to name just a few), the landscape becomes even more dense. That's before we even start to consider each organisation's specific challenges. Technical debt, cost constraints, and rapidly evolving cyber threats are just the tip of the iceberg. Plus, customer expectations are constantly changing. So, too, must financial services if they are to deliver what customers want and need.

Nowadays, digital is at the heart of achieving that, creating exciting new opportunities to differentiate, innovate, and grow and retain a bigger market share. But, of course, this new digital world also exposes financial organisations to even greater critical risk of systems disaster, data breaches and other equally unpalatable scenarios. So, firms must modernise from a commercial perspective, while also ensuring that every touch point across the business is robust and safeguarded. Faced with such an intricate web of challenges, where on earth do we begin?

Effective resilience planning begins by asking the right questions

In fact, the starting point is a change of mindset. It's important to appreciate that achieving real operational resilience is not just IT's job. This is a business-wide challenge, so tackling it must start at the top, with strong C-suite leadership and the right focus. And that focus should be, first and foremost, on identifying the critically important business services that need to be protected. Fundamentally, we should be asking: what are the scenarios that would truly risk breaking our implicit, and explicit, contract with our customers?

In my experience, answering that question is more difficult than we might think. Typically, if I were to approach ten people in your business and pose the same question, the chances are that I would get ten different answers. Each of those stakeholders will have their own perception of what constitutes an important business service, based on their own role, experience and priorities. That doesn't really help anyone, because tackling a roadmap as complex and crucial as this requires an end-to-end understanding not just of where the real risks lie, but of how they interlink. Can we fully map dependencies between, for example, digital payments and data protection? Who are the owners and stakeholders of those systems? How do they (and their systems) talk to each other? Do we have a clear picture of exactly where a critical risk may be triggered? Crucially, what level of disruption can we tolerate before real harm might occur?

To answer these questions, it's essential to draw back from departmental detail and cast an objective, informed lens across the entire organisational ecosystem. That responsibility lies firmly in the hands of the CEO and board. It must be the first step because, without that intelligence, designing a meaningful, sustainable operational resilience roadmap simply isn't possible.

From operational resilience to enterprise resilience: a strategic shift

Achieving that rigorous focus on the resilience headlines is the starting point. The second challenge is how to predict and defend against critical risks? Once the business has agreed its vision and objectives for operational resilience, the next step is to map out the strategy, process, tooling, policy, and operating model to support those. This is where a deep dive across, up and down the business and its supply chain is needed. It is crucial to build a comprehensive picture of not just the technology, infrastructure, and systems, but the people and ways of working that may impact a service. This then forms the scope of the operational resilience strategy, framework, and delivery.

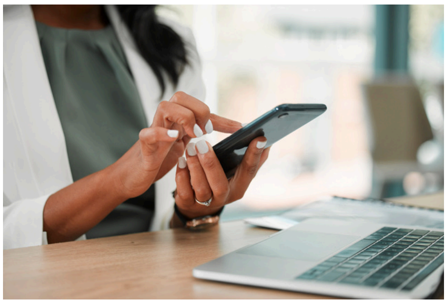
At Mason Advisory, we often talk to our clients about 'Enterprise Resilience Management'. It's our way of describing an approach that integrates resilience into the core of your business. I say "your" because, of course, every business is different. While all financial service organisations should, quite rightly, be FCA and DORA compliant, your organisation is also likely to face your own set of unique challenges in the resilience arena and beyond. So, it's important to design an operating model and roadmap that aligns to your situation and capabilities across governance, people, process, technology and data. The big picture can be overwhelming, but underpinning the end goal with a manageable, iterative roadmap turns what might seem impossible into something that is realistic and feasible. Across all of this, it can be invaluable to invite an independent perspective. A fresh set of eyes and the right track record of experience will help to cut through the fog and bring clarity and purpose to the resilience landscape.

At the beginning of this article, I mentioned the importance of a change of mindset, where operational resilience becomes a business concern, not just a technology concern. There’s another shift in thinking that we should embrace. So many organisations are dealing with multiple IT and technology conundrums as they race to deliver what tomorrow’s customers want. In fact, all the foundational work that goes into understanding the resilience landscape is the same work that will drive a deeper understanding of technology’s capacity to enable the business. And that understanding is exactly what will equip the business to respond rapidly to market changes, new customer demands and emerging threats, as well as the regulatory landscape.

All of this points to one key principle: operational resilience (or enterprise resilience, to coin our term) is not a finite activity. In an ever-changing world, the organisation that assumes there is an end point is the organisation that makes itself vulnerable. So, starting from the C-Suite and cascading through the entire enterprise, this is a continuous improvement roadmap that should be at the top of the strategic agenda and embedded into the organisational DNA. It is only when that is achieved that a business can truly call itself resilient and start to maximise the benefits that come out of that.

Jon and his team at Mason Advisory offer decades of experience in tackling operational resilience from an enterprise-wide perspective. If this is an area where you need help, we can offer an informal, confidential discussion of your challenges.

To find out how we can support you, use our website to make an enquiry, email us at fsi@masonadvisory.com, or call us on +44 (0)333 301 0093.



Insight overview

Insight 2 of 3 - Building enterprise-wide operational resilience: the top priorities (plus mistakes to avoid)

Moving from siloed operational resilience to sustainable enterprise resilience requires a holistic approach across strategy, people, process, technology, and the supply chain, writes Kaustubh Ambavanekar.

In the first of our operational resilience article set, my colleague, Jon De'Ath, outlined the importance of embracing operational resilience as a continuous, enterprise-wide endeavour. Of course (and as he points out) updated FCA and PRA regulations, plus the introduction of DORA, are key drivers behind a double-down focus on operational resilience across financial services. But, while compliance is crucial, it is just the start of tackling a complex web of considerations when it comes to protecting the business and its customers.

In today's digitally driven world, the process of building, mapping, testing and validating scenarios, tolerances, and strategies to mitigate constantly evolving threats is a real challenge. It is certainly true that most financial services organisations are already on an operational resilience journey of some kind. But how can we be sure that it is the right roadmap, tackling the right priorities in the right order, to ensure that resilience is integrated into the organisational ecosystem?

Mason Advisory has been deeply involved in this space for some years now. In our experience, the reality is that many organisations still struggle to achieve clarity across what those priorities are and where resources should be focused. In the resilience arena, with all its dependencies, it is easy to become overwhelmed and lose sight of the business-critical headlines. That is why we have developed Mason Advisory's Operational Resilience Management Framework. It is designed to leverage existing governance, compliance, and risk capabilities and ensure that every key resilience category is addressed in a holistic, embedded, and interconnected way.

Joining the dots between strategy, people, process, and technology

It is important to be clear that, when I talk about a holistic approach, that does not mean trying to address every area of operational resilience all at once! Yes, they are all connected. However, introducing a logical flow to the resilience roadmap drives clarity and purpose, while ensuring that no vital balls are dropped along the way.

The first priority is articulating a strategic perspective so that business continuity, disaster recovery, and enterprise risk management come together to deliver overall business resilience. Of course, the business depends on its operations to function – so this is what should receive attention next. As my colleague, Jon, points out in his article, typical trip-ups include inaccurately identifying what represents a genuinely critical tolerance. Considerable resources are needed to model, test, and mitigate multiple scenarios across IT governance, risk, compliance, outsourcing and the third-party supply chain. So, understanding where to focus those resources is crucial to avoid confusion, overwork, and unnecessary exposure to threats.

Then, we must examine the technology infrastructure. Do we understand where the real vulnerabilities lie? Do we have a robust plan for ongoing technology resilience and, if the worst happens, recovery? Where does IT service sit in this landscape? This leads us into data and cyber considerations. How are we safeguarding our information security, availability, backup, and recovery? Do we understand how data and cyber threats are evolving? Can we say, with confidence, that we are geared up to pivot and respond, at speed, should those threats affect our delivery?

It quickly becomes clear that operational resilience demands a combined strategic, operational, and technical perspective. But there is one more link in the chain: people. In my experience, this is the most commonly underestimated area when driving enterprise-wide operational resilience. The workforce plays a crucial role in bridging the gap between business and technology. Even if the priorities described above are tackled effectively, it is essential to ensure that the resilience characteristics are developed at an individual level and that the organisational culture empowers the right mindset and behaviours to drive enterprise-wide resilience. Consider, for example, continuity planning. If people that set up and or manage operational environments aren't able to maintain, fix, manage or failover operational systems and the data in them when needed. They might have left the organisation, might be retired, or of course they may themselves have been affected by the cause of the disruption. Organisations should consider building cross functional multi-disciplinary teams with different functional expertise working towards a common goal. If a specific scenario, such as a disastrous outage, affects one team, which other business functions might also be impacted by that downtime? These are just some of many possible examples, but they demonstrate the importance of fostering a lean, agile culture, ensuring that the resilience characteristics are developed at an individual level and that people in your organisation have developed a resilient mindset and cultivate a resilient behaviour where, should such scenarios happen, people are geared up to continue delivering through shared knowledge, localised autonomy (within the right governance framework, of course), and confidence in decisions and actions that align with the overall direction of travel.

Three common operational resilience mistakes to steer clear of

Just like any mature business practice, building a robust resilience capability is not just about investing in the right priorities. It is also about understanding the potential pitfalls that will at best divert attention away from what we should be doing, and at worst may compromise the entire resilience landscape. In my experience, there are three headlines that any technology or IT leader should keep in mind:

1: Move beyond an exclusively top-down view

Of course, it is the job of leaders to lead, and so it is natural for initiatives including operational resilience to be driven from the top. However, this can become problematic if the view from above excludes all other perspectives. A more holistic, horizontal mindset is needed to ensure that the interdependencies that connect the business (and, indeed, the supply chain and the customer) are comprehensively mapped, tested, and validated. A broad, deep, impartial, and extremely thorough approach is needed here, alongside intelligence gathered from multiple stakeholder experiences, expertise, and viewpoints to ensure that the true risks are uncovered and mitigated.

2: Don't take on more than is manageable

The process outlined above might uncover hundreds of potential resilience pitfalls, but it is unlikely that every single one represents a truly disastrous scenario. So, it is important to identify the most pressing issues to streamline the effort. I have seen many scenarios where an attempt to cover every base at once actually achieves the opposite – nothing receives the attention it deserves. Within the five priority areas mentioned earlier, every business must decide: which risks are the most urgent for us and our customers? What are the scenarios that would truly render us inoperable, vulnerable, or at risk of fines or sanctions? These are the areas demanding an immediate laser focus. Once the strategy, tactics and tooling are in place to mitigate those scenarios, the approach can be expanded until, eventually, resilience is established not just internally, but across the entire organisational ecosystem. Which leads me nicely into:

3: Ensure the supply chain is on your side

The supply chain is any business's lifeblood. We all know this. Nonetheless, it is a common challenge to effectively onboard third-party suppliers and align their ways of working with your organisation's operational resilience framework. Perhaps surprisingly, the trickiest area of aligning suppliers' roles to organisational resilience is cultural. Yes, operational risks, scenarios and mitigations must be explored. But when crunch time comes, it's the relationship you have developed with your suppliers that will enable a fast recovery. Aligning cultures and building out that relationship is a good place from which to start pro-active conversations with third parties. And that is an important component in the journey towards full Enterprise Resilience, as I will explore in my next article, which you can read now.

Whether you're starting out on your resilience roadmap or fully in-flight, an independent perspective can be invaluable to validate the approach. Mason Advisory has extensive experience of aligning activities within a controlled framework, moving you from Operational to Enterprise Resilience and ensuring every base is covered in the right order. You can enquire via our website, email us at fsi@masonadvisory.com, or call us on +44 (0)333 301 0093.

Insight overview

masonadvisory

Insight 3 of 3 - Establishing end-to-end operational resilience capability is as much about culture as process

When it comes to operational resilience, embedding the right culture across the entire organisational ecosystem is an essential endeavour, as Kaustubh Ambavanekar explains.

Establishing end-to-end operational resilience capability is as much about culture as process

The first two articles in this Operational Resilience series set the scene for a mindset shift from Operational Resilience to what we at Mason Advisory call 'Enterprise Resilience'. The term reflects the importance of building resilience into the fabric of the organisation and across the supply chain, from third party suppliers, through internal stakeholders, and out to the customer.

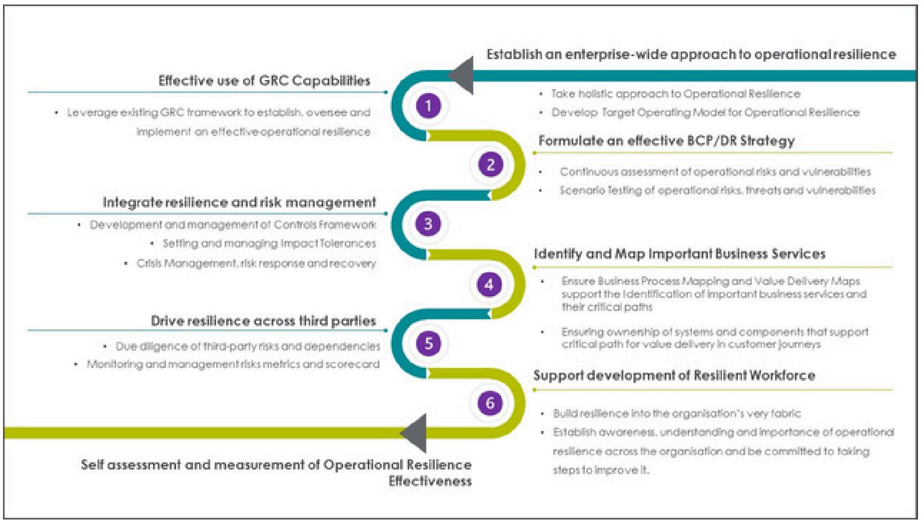
My previous article outlined how a strong, prioritised Enterprise Resilience Management framework keeps the roadmap on track, ensuring that effort and resources are targeted to the right areas at the right time. I explored the importance of establishing a resilient internal culture that considers issues like continuity planning and encourages a lean, agile approach, enabling your people to function effectively, even if disruption or disaster strike. And I touched briefly on the importance of looping the third-party supply chain into the approach. Now, I would like to delve deeper into that last notion by examining the challenges that organisations typically face when attempting to align internal ways of working with external stakeholders.

In fact, in my experience, most organisations have more resilience capabilities in their armoury than they might think.

Depending on the maturity level, it is comparatively rare to come across an organisation that has not already thought about, for example, their Governance, Risk and Compliance (GRC) framework, or some sort of Disaster Recovery plan. This is good news, providing the foundations from which to build a full resilience capability. Where things tend to come unstuck is in connecting all of the components in an integrated way. This is partly a question of mapping a strategic resilience framework and partly a process of designing and delivering the right architecture and roadmap. But, to bring all of this together, there is also cultural work to be done to establish an understanding of why resilience matters and a commitment to continuous improvement across all stakeholders.

Designing an Operational Resilience roadmap that plays to your strengths

My last article described the strategic framework that should connect IT with the business to establish Enterprise Resilience. Now, let's explore an approach on building an Operational Resilience roadmap leveraging current capabilities. This will vary depending on organisational maturity, the effectiveness of existing capabilities, and where the business is on its resilience journey. But a typical example of building a robust operational resilience roadmap might look like this:



Establish an enterprise-wide approach to operational resilience
• Take holistic approach to Operational Resilience
• Develop Target Operating Model for Operational Resilience
1
Effective use of GRC Capabilities
• Leverage existing GRC framework to establish, oversee and implement an effective operational resilience
2
Formulate an effective BCP/DR Strategy
• Continuous assessment of operational risks and vulnerabilities
• Scenario Testing of operational risks, threats and vulnerabilities
3
Integrate resilience and risk management
• Development and management of Controls Framework
• Setting and managing Impact Tolerances
• Crisis Management, risk response and recovery
4
Identify and Map Important Business Services
• Ensure Business Process Mapping and Value Delivery Maps support the Identification of Important business services and their critical paths
• Ensuring ownership of systems and components that support critical path for value delivery in customer journeys
5
Drive resilience across third parties
• Due diligence of third-party risks and dependencies
• Monitoring and management risks metrics and scorecard
6
Support development of Resilient Workforce
• Build resilience into the organisation's very fabric
• Establish awareness, understanding and importance of operational resilience across the organisation and be committed to taking steps to improve it.
Self assessment and measurement of Operational Resilience Effectiveness

Figure 1 - Roadmap and Key Principles

This kind of logically sequenced roadmap allows the business to achieve momentum by leveraging the best of what is already there (for example, GRC capabilities). That, in turn, sets the stage to build on a strong foundation by revisiting areas like Business Continuity and Disaster Recovery plan in the context of the latest resilience landscape, including changing regulations. Next, it makes sense to focus on integrating continuity and recovery into existing risk and resilience management functions, for a seamless approach. Having connected the main resilience capabilities, building accountability and ownership across those responsible for important business services and their critical paths embeds the approach in a sustainable way. How leaders achieve this will depend in no small part on the established organisational culture, ways of working and leadership style. But it must be understood that cultural management is an ongoing journey, not simply a discrete task. In summary, leaders must work with their people to ensure that resilience is being built into the organisation's DNA – through values, behaviours, and ways of working – every day.

Extending the approach to third party suppliers

All of the above is essentially within the organisation's control – although many businesses find that validating their approach with the benefit of an independent, expert, impartial view brings valuable clarity and focus. However, when we look at the wider ecosystem, factors become more unpredictable. Suppliers have their own cultures which will vary considerably according to the respective industry, the nature of the product or service, and indeed the supplier's own incoming stakeholder chains and influences.

So, how do we align? The key is in establishing clarity, parameters, communication, and motivation. Ultimately, it starts with a conversation. If there is an opportunity to build that conversation into initial procurement, engagement, and onboarding, then all the better. If the relationship is already established, introducing a debate which effectively seeks to revisit the supplier/client relationship might be harder. But, in either case, it must be done. Because, if your supply chain does not align to your resilience framework, neither party is truly resilient nor protected. So, the key is in demonstrating the benefits of a joined-up approach, providing a clear and manageable framework that your suppliers can dovetail into, maintaining a transparent dialogue, and supporting that with refreshed contractual conditions where feasible. Plus, remember that this is not just about how your supplier engages with your business. It is also about how your business operates with its suppliers, and this is where revisiting and refreshing the resilience approach is of as much benefit to them as to you.

Finally, let's not forget that all of this must also extend to the other end of the ecosystem: the customer. For financial services organisations, multiple scenarios need to be considered, tested, and mitigated, especially in light of new FCA, PRA and DORA regulations which will be non-negotiable come March 2025. Every financial organisation needs to ask probing questions. What are our customers' tolerance levels? How would we communicate with and reassure them in the event of an outage? How can we reassure them that their data (and, or course, their money) is secure? What do they need from us to trust us? The answers to questions like these not only help to target efforts to the right resilience initiatives. They also allow technology leaders to do important work, ensuring that the architecture, operating model and capabilities are geared up to connect the supply chain, internal operations, and the customer in a holistic way.

None of this is easy, and it will take time. All of it, however, is achievable. Plus, as my colleague, Jon De'Ath, explains in the first article of this series, this is not a finite activity but a journey of continuous review and improvement. Because the world of digital threats is evolving. So, every financial services organisation must evolve alongside, to ensure that the business delivers what is needed, not just to protect itself, but to attract, grow and retain that all-important customer base.

Mason Advisory has long experiences of helping financial organisations – from multi-national banks to regional building societies – to tackle their Operational Resilience challenges. If you are concerned about being ready for new regulatory compliance, or simply want to initiate or revisit an internal resilience strategy, talk to us. You can enquire via our website, email us at fsi@masonadvisory.com, or call us on +44 (0)333 301 0093.

Contacts

Jon De'Ath
Managing Director
email: fsi@masonadvisory.com

Mike Kingston
Managing Consultant
email: fsi@masonadvisory.com

Kaustubh Ambavanekar
Principal Consultant
email: fsi@masonadvisory.com

About Mason Advisory

Mason Advisory has offices in Manchester and London and employs over 100 staff, with plans to continue its expansion. We enable organisations to deliver value through digital & technology transformation, solving complex business challenges, and helping clients set strategy through the intelligent use of IT resources including architecture, cyber, data, digital, operating model and organisational design, service management, and sourcing. We operate in sectors such as financial services and insurance, legal and law, government, health and social care, emergency services, retail, FMCG, transport, and not-for-profit.

Contact us

To get in touch, please email contact@masonadvisory.com or call +44 333 301 0093

OFFICES

MANCHESTER
Landmark
St Peter's Square
1 Oxford Street
Manchester
M1 4PB

LONDON
Bush House
North West Wing
Aldwych
London
WC2B 4PJ

Studio 202
77 Coleman Street
London
EC2R 5BJ

masonadvisory