**mason**advisory
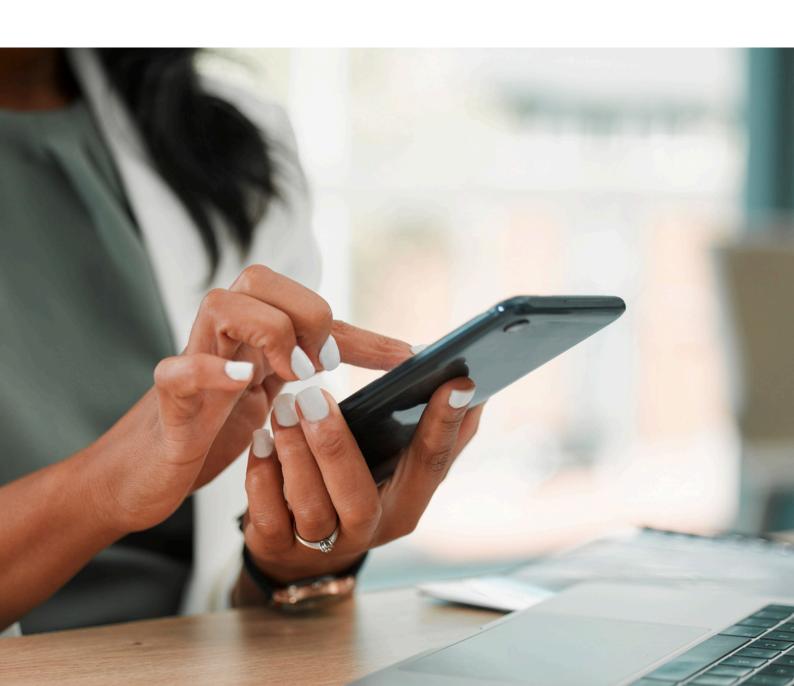
# Insight 1 of 3 - The right resilience roadmap starts with the right questions

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.

# Author

Jon De'Ath
Managing Director
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