Insight overview

masonadvisory

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.

Author

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