bmc

Report in collaboration with

FStech

FROM HYPE TO IMPLEMENTATION: UNRAVELLING THE COMPLEXITIES OF OPERATIONAL RESILIENCE IN MODERN FINANCIAL SERVICES

INTRODUCTION

The financial services landscape is evolving rapidly, with operational resilience emerging as a critical priority for institutions. Systemically important financial institutions (FSIs) often labelled "too big to fail," must manage disruptions that could ripple across the global financial system. In response, they face pressure to fortify operations against risks and comply with new regulatory frameworks in the UK, EU, and beyond.

Many FSIs remain unprepared for the complex demands of upcoming operational resilience regulations, and do not have adequate reporting structures in place to demonstrate the operational resilience strategies and processes they deploy on a daily basis to protect their customers and business needs. A recent survey by FStech and BMC Software, involving 100 EMEA based financial professionals, paints an intriguing picture of industry attitudes towards operational resilience as key decision makers look to balance regulatory reporting requirements with those internal strategies and processes.

Rather than regulation driving operational resiliency, operational resiliency is primarily dealt with as an internal process by FSIs. While institutions clearly understand the risks and are focused on implementing effective operational resilience strategies, this internal focus risks leading FSIs to non-compliance regardless of how successful they are at avoiding outages or defending against cyberattacks.

As such, what appears to be slow progress towards preparedness on the surface is instead more likely to be a 'wait-and-see' approach, where FSIs believe that regulations such as the EU's Digital Operational Resilience Act (DORA) and the PRA's operational resilience policy (PS21/3) do not require new processes and are instead an iteration of existing Governance, Risk, and Compliance (GRC) demands.

But while FSIs have their own stringent processes, these regulations are not designed to be a 'box ticking' exercise; they have been created to ensure that FSIs have the correct processes and governance to deliver secure, resilient systemic financial services.

However, industry frustration towards a lack of clarity around those regulatory requirements likely means that the real demands of these looming regulations will only reveal themselves once FSIs start getting audited and hit with non-compliance.

The following report shows a financial services industry where key decision makers are striving to meet their operational resilience needs as a primary objective through appropriate investment, operational alignment and cutting-edge technologies, while also attempting to balance those objectives with the demands of the regulator – even if it means potentially missing key reporting deadlines.

KEY FINDINGS:

1. Preparedness Gap: Only 12 per cent of FSIs are fully prepared for new regulations, while 49 per cent remain unready, with less than a year to comply with DORA and the PRA's operational resilience policies.

2. Lack of Clarity: 59 per cent of respondents find regulatory guidance unclear, making it difficult to set impact tolerances and manage third-party risks effectively.

3. Slow Compliance: 78 per cent of FSIs estimate they need 6 to 36 months to achieve compliance, far exceeding regulatory deadlines.

4. Investment Priorities: FSIs are focusing on documentation (26 per cent), technology upgrades (19 per cent), and cybersecurity (13 per cent), but areas like business continuity planning (6 per cent) remain underfunded.

5. Technology as an Enabler: RPA (44 per cent), automation tools (41 per cent), and machine learning (37 per cent) are driving compliance and risk management, while emerging tech like Generative AI (30 per cent) and Cloud Native technologies (32 per cent) are shaping future resilience strategies.

REGULATORY READINESS

In terms of readiness to meet regulatory deadlines, only 12 per cent of institutions are fully prepared, while 49 per cent are not ready. This latter figure includes nearly 10 per cent of respondents who have taken no steps to prepare. With mere months until key deadlines, including the EU's DORA (17 January 2025) and the PRA's (PS21/3) (31 March 2025), these figures should not necessarily be taken as an alarming admission of operational ineptness – rather that FSIs' primary concerns lie with their day-to-day business and demonstrating that compliance comes as a lower priority.

Being compliant and demonstrating compliance are two entirely different complications, and FSIs face multiple hurdles in compliance – particularly surrounding governance and accountability (45 per cent), incident reporting (42 per cent), and third-party risk management (41 per cent). These issues are compounded by the complexity and scope of the new regulations, which require overhauls in governance, technology, and reporting.

Furthermore, 59 per cent of respondents expressed frustration over unclear regulatory guidance, making it difficult to translate broad principles into actionable steps. This lack of clarity – explored in more depth later in the report – complicates compliance and increases uncertainty about what regulators expect, especially in setting impact tolerances and managing third-party risks.

As internal processes continue to drive operational strategies and processes, these challenges are not surprising. The complexity of ensuring ownership and accountability for such a critical topic is significant, and many firms have shown gaps between their own internal processes and regulatory reporting. Additionally, fragmented and sometimes ambiguous guidance across regulations can exacerbate these challenges, leaving key decision makers uncertain about how to prioritise and allocate resources in a manner that meets compliance requirements.

ROADMAP TO COMPLIANCE

One notable finding is that 78 per cent of respondents estimate they need six to 36 months to achieve regulatory compliance, far exceeding regulatory deadlines. Despite having comprehensive processes in place, this timeline stretches far beyond the deadlines set by both DORA and the PRA and lends credence to the viewpoint that firms are adopting a 'wait-and-see' approach to the realities of how these regulations will be applied.

This however is a potentially risky approach from a regulatory standpoint and could lead to regulatory audits. While existing internal frameworks may be fit for their own purpose, the survey highlights the tension between the increasing complexity of regulations and the insufficient clarity provided to help firms meet these expectations.

To achieve compliance in a timely manner, FSIs must transform their reporting processes to demonstrate their operational resilience strategies in a compliant manner. The survey reflects a market sentiment that regulatory bodies should play a more active role in providing clear, actionable guidance if they are to help firms navigate these multifaceted requirements within the tight deadlines.

It is also worth noting that the inverse situation is also potentially true – being compliant does not necessarily mean that organisations have a fully baked and effective operational resilience strategy, process and plan. If they have just treated it as a box ticking exercise to maintain compliance, they risk an even worse outcome than an audit.

As an example, a firm can demonstrate compliance with ISO27001 information security practices on the day of assessment – with assets stored securely; computers and terminals logged off when not in use; printers restricted to authorised users etc. – but this does not necessarily mean that these practices are adhered to strictly on a day-to-day basis or always recognised by staff. A compliance certificate is worth less than the paper it is printed on if one lapse in concentration leads to a business-critical outage.

That said, it is reassuring to see that most financial institutions surveyed have robust operational resilience processes in place, but it remains to be seen how long it will take them to marry those processes with the demonstrable requirements of regulations like DORA and PS21/3.

OPERATIONAL INVESTMENT

FSIs are directing their investments towards specific areas to build operational resilience, but the survey shows these efforts may not be comprehensive enough. Most investment is focused on documentation and reporting capabilities (26 per cent), reflecting the need for clear audit trails to show compliance, and a requirement to maintain proper records in the event of an operational disruption.

Technology upgrades (19 per cent) are another priority, as institutions recognise the need to modernise legacy systems and enhance operational capabilities. These upgrades are essential as financial services increasingly rely on digital platforms that demand robust, real-time risk management.

Cybersecurity (13 per cent) is also a key investment area, as FSIs look to protect against growing cyber threats. However, focusing solely on these foundational areas may leave gaps, such as in business continuity planning (only 6 per cent investment), which is critical for a comprehensive operational resilience strategy.

Without a comprehensive approach to operational resilience that includes all aspects of risk management, institutions could find themselves exposed to vulnerabilities.

OPERATIONAL ALIGNMENT

Achieving operational resilience requires significant internal alignment, yet many FSIs encounter significant barriers. Compliance (50 per cent) and senior management buy-in (44 per cent) are the biggest challenges. Without clear leadership support and resource allocation, resilience efforts can stall. Aligning human resources (37 per cent) and operations (38 per cent) also remains difficult, especially in siloed organisations.

Firms that identify senior management buy-in as a major issue, may risk being unclear around the ultimate ownership of the operational resilience strategy and processes – as demonstrated by the 45 per cent of respondents who identified governance and accountability as a challenge to their regulatory compliance. Operational resilience is a critical item on the list of business priorities, and an owner within the business should be championing its importance as a point-of-reference for both internal staff and for the regulator.

This lack of clear ownership stands in contrast to regulatory requirements, which demand that figures like audit and risk committees, chief information security officers and chief risk officers report operational resilience information to the regulator. This creates a potential challenge as a successful operational resilience strategy requires buy-in from across the business, with IT and specific business units required to make their delivered services resilient in a fashion that meets requirements.

Budget constraints and cultural issues are two additional significant barriers to alignment. Demonstrating operational resilience is often seen as a compliance cost rather than a strategic priority, and this view can stifle efforts to secure leadership buy-in or cross-departmental collaboration, both of which are critical for success. The negative impact of operational resilience costs can be a cultural strain, with different decision makers wanting to have an opinion on direction without the ownership or cost sitting within their department.

Addressing these challenges requires a concerted effort to foster collaboration across departments, alongside a strong commitment from leadership. Securing necessary budget for previously discussed technology upgrades and embedding resilience into the strategic priorities of the institution is vital for aligning operations with regulatory requirements and long-term sustainability.

OPERATIONAL CLARITY

Financial institutions are grappling with the complexity of the new regulations, particularly around understanding, and implementing key requirements. Some 59 per cent of respondents mentioned that regulatory guidance lacks sufficient clarity, making it difficult to translate these requirements into actionable plans.

One of the most critical challenges lies in setting impact tolerances, which define how much disruption an institution's important business services can withstand before causing severe harm to the organisation or the broader financial system.

Impact tolerances are central to operational resilience, and guide decision-making during crises to ensure that allocated resources sufficiently protect the most critical services and maintain operational continuity. However, 21 per cent of FSIs struggle to set these tolerances due to difficulties in quantifying disruption across interconnected services.

Institutions often face challenges when attempting to gather reliable data, accurately model potential disruptions, and balance regulatory requirements with their operational realities. Additionally, the process of defining acceptable levels of risk can vary depending on the institution's size, market, and geographic footprint, adding further complexity. Some institutions may struggle in this regard due to insufficient staff training or skills, or due to a lack of visibility around the data required to analyse.

Compounding these difficulties is the challenge of mapping and testing important business services. Mapping requires identifying all critical business services, understanding their dependencies, and assessing how disruptions would impact the overall operation. Testing, on the other hand, involves simulating crisis scenarios to ensure that these services can continue functioning within the defined impact tolerances. Many firms struggle with these tasks, due, in part, to insufficient regulatory guidance, a lack of robust internal strategies and the absence of the correct technologies.

Regular testing is essential for ensuring that institutions can stay within their impact tolerances, but without clear frameworks, many FSIs are left uncertain about how to proceed.

59%

OF RESPONDENTS MENTIONED THAT REGULATORY GUIDANCE LACKS SUFFICIENT CLARITY, MAKING IT DIFFICULT TO TRANSLATE THESE REQUIREMENTS INTO ACTIONABLE PLANS.

This is borne out by only 15 per cent of FSIs expressing high confidence in their ability to meet these thresholds. This low level of confidence suggests a broader issue: firms are not fully integrating impact tolerance concepts into their risk management frameworks.

Risk management is an existing process of every FSI and is so ingrained that it often works at an abstracted level that is baked into day-to-day business functions without active consideration. By contrast, operational resilience impact tolerance is a new adjacent concept that requires greater granularity in what is managed, how it is tracked and what is considered as part of the impact.

For many, the lack of comprehensive testing, coupled with unclear regulatory expectations, makes it difficult to ensure they are adequately prepared for worst-case scenarios.

Historically, risk management has considered the 'what' and 'when' but not the 'by whom'. The sudden shift to remote working in 2020 demonstrated to many FSIs that they were unprepared to deliver services when staff had to work from home, and this exposed multiple resilience issues where traditional external access to key systems just wasn't designed for the scenario. Such once-in-a-generation global moments are unlikely to occur again in the near future, but the episode demonstrates the much broader activities that impact tolerances must consider compared to traditional GRC approaches.

TECHNOLOGY AS AN ENABLER

As operational resilience demands increase, FSIs are turning to technology to ease the burden of compliance. Automation, real-time risk monitoring, and data insights help institutions manage risks more efficiently.

As operational resilience demands increase, FSIs are increasingly turning to technology to reduce the burden of compliance and enhance their resilience capabilities. Automation, real-time risk monitoring, and data insights can all play a vital role in helping institutions manage risks more efficiently and effectively.

Robotic Process Automation (RPA) (44 per cent) is at the forefront of these efforts, allowing institutions to automate routine, repetitive tasks such as data collection, reporting, and compliance checks. RPA helps FSIs automate compliance activities and can support improved resilience of the underlying services with fewer resources.

Automation and orchestration tools (41 per cent) provide another layer of support by enabling institutions to automate more sophisticated processes that involve multiple systems and departments. These tools help manage operational risks in real-time by coordinating responses across different areas of the organisation, ensuring that disruptions are handled quickly and efficiently. By reducing the reliance on manual interventions during crises, automation and orchestration tools minimise downtime and allow for a more agile response to potential operational failures.

Similarly, Machine Learning and Analytics (37 per cent) are becoming critical tools for real-time monitoring and risk assessment. By analysing vast amounts of data, these technologies can identify emerging threats, predict potential disruptions, and provide actionable insights. This predictive capability allows institutions to move from reactive to proactive risk management, reducing the operational strain on human teams and enabling faster, data-driven decisions.

Looking ahead, emerging technologies such as Generative AI (30 per cent) and Cloud Native solutions (32 per cent) are gaining traction for their potential to transform how institutions manage operational resilience. Generative AI can enhance decision-making processes by quickly generating insights from complex data, while cloud-native solutions offer greater flexibility and scalability, allowing institutions to respond to disruptions without being constrained by traditional, on-premises infrastructure. These technologies are enabling FSIs to build more adaptive and future-proof resilience strategies, further reducing the strain on internal resources.

By automating routine tasks, enhancing real-time risk management, and offering scalable solutions, FSIs can significantly reduce the operational burden that they face while navigating increasingly complex regulatory environments. Technology is no longer just an enabler – it is essential to achieving operational resilience in today's financial landscape.

CONCLUSION

The financial services sector faces significant challenges in preparing for operational resilience regulations. While the survey highlights encouraging investment in documentation, technology upgrades, and cybersecurity, many FSIs are still unprepared for the fast-approaching deadlines and indicates that many are adopting a 'wait-and-see' approach to how the regulations will be applied. But while regulatory compliance is a chief concern, the report demonstrates that achieving operational resilience requires not just technological investments, but also organisational alignment, leadership support, and clear regulatory guidance.

The consequences of inadequate preparation extends far beyond regulatory penalties. Institutions that fail to adapt may find themselves at a competitive disadvantage in an increasingly digital financial landscape. To remain resilient, FSIs must treat operational resilience not as a compliance cost, but as a strategic imperative for long-term sustainability and competitive edge.

bmc

in collaboration with

FStech