Unsplash © Ksenia Makagonova

Emerging operational resilience trends

In March 2021 the Bank of England, Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA) published their final suite of documents on Operational Resilience (‘Final Policy’). The Final Policy documents set out the expectations and outcomes regulated firms will need to adhere to in order to establish and maintain resilience of their Important Business Services.

The U.K. regulators expect that for regulated firms to be ‘operationally resilient’ they should, as an outcome, be able to ‘prevent disruption occurring to the extent practicable; adapt systems and processes to continue to provide services and functions in the event of an incident; return to normal running promptly when a disruption is over; and learn and evolve from both incidents and near misses’.

Therefore, regulated firms will need to ensure that they have set out and finalised their approaches to ‘severe but plausible’ scenarios, identified and mapped their Important Business Services, and set their impact tolerances by the end of March 2022. There will be a three-year transition period from March 2022 until March 2025 where regulated firms will need to ensure full adherence to the Operational Resilience rules and outcomes.

Wavestone continues to support our regulated clients within the U.K. with their Operational Resilience activities, and as a result we have started to see a number of common implementation trends emerging. The following 6 key trends summarise the consistent themes that we are seeing emerging across Operational Resilience within the U.K.

Trend #1: The need for independent assurance

A number of regulated firms first developed their ‘response strategies’ during policy development, and for some firms, these were completed as early as 2018.

This has meant that some implementation strategies have remained fairly high-level or conceptual with the detailed ‘how to implement’ approach still being determined well into 2021.

Too often we have seen that some firms have struggled with the operational challenge in translating early ‘conceptual’ strategies into actionable plans, as well as dealing with organisational and functional silos that are further compounded by pre-existing legacy technology and data quality issues.

What can be done?

As the March 2022 deadline soon approaches it will be important for firms to undertake a full review and assurance of current approaches to their identification of Important Business Services, scenarios, and mapping exercises prior to the March 2022 deadline.

The benefit of an independent assurance will provide an external view across all the key elements as well as assess the robustness of the internal analysis against the expectations and outcomes set by the UK regulators.

Trend #2: Building a multi-disciplinary engagement model

Operational resilience touches upon a number of areas that blur the lines between multiple traditional risk disciplines and so requires a different approach to managing resilience risk.

We are seeing regulated firms looking at augmenting the engagement model with a focus on realigning risk roles and responsibilities across the

three lines of defence as well as addressing risk frameworks, risk appetite statements, and underlying policies, processes, and procedures to ensure that multiple risk disciplines are operating effectively in respect to resilience.

What can be done?

Resilience is an outcome that will require clear accountability where the accountability lines may straddle across different areas rather than be fully demarcated.

Focusing on building a holistic accountability and engagement model across the three lines of defence to effectively demonstrate that outcomes are being achieved will be critical for internal and external reporting accountability.

In time, such an approach will require a break down in some of the historically siloed activities or functions in order to have a read across the risk disciplines.

Trend #3: The perennial legacy infrastructure problem

> It is inevitable that there will always be a degree of legacy technology within an environment. This is perfectly manageable so long as that technology is still maintainable and does not introduce significant risk or affect service delivery to customers or end-users.
>
> However, within the context of resilience, this justification simply does not hold up to scrutiny. It will not be enough to meet the expected outcomes.

What can be done?

Legacy technology and technical debt obsolescence require a full assessment to determine where Important Business Service touches upon or relies upon obsolescent (end of life or end of support) applications or hardware.

Therefore, a core activity within the mapping of Important Business Services will be to identify and mitigate obsolescence within the technology environment that affects or has the likelihood to affect resilience, and once identified to address mitigation to flatten the associated risk profile.

Trend #4: Consistent governance model

During 2020/2021 the concept of 'resilience' has taken on more of a critical focus for regulators outside of the UK, in particular the:

Bank of International Settlement (BIS) '*Principles for Operational Resilience*'

European Commission's '*Digital Operational Resilience Act*' ("DORA"), which aims to harmonise digital operational resilience rules for financial organisations in the EU

Federal Reserve (Fed), Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC) published a *joint paper* outlining sound practices to strengthen operational resilience within the United States.

Hong Kong Monetary Authority's *'Principles for Operational Resilience and Revised Principles for Sound Management of Operational Risk'*

Monetary Authority of Singapore (MAS) *'Ensuring Safe Management and Operational Resilience of the Financial Sector'*

However, all is not the same and there are subtle variations between policies. For example, the definition of 'resilience,' 'important' and 'critical' operations, and what is deemed to be a 'material' or 'critical' outsourcing globally present certain governance challenges for firms that operate within key financial jurisdictions; as well as challenges in how to structure a global resilience operating model approach to avoid operational inefficiencies are emerging for multinational financial services firms.

What can be done?

It will be important to consider a coordinated and overarching approach to a global operational resilience operating model.

The Board and Senior Managers are ultimately accountable and responsible and therefore firms will need to ensure that competency, capability, and capacity of individuals are in place at each stage of the operational resilience lifecycle as well as looking to ensure that local and regional compliance and reporting are undertaken in an efficient and coordinated way.

Trend #5: Data Quality, Tooling, and Reporting

> We have seen that management information (MI) and tooling remains a complex issue for firms, which is largely due to legacy functional and data siloes across organisations but also the lack of rationalisation of incumbent tooling systems which inhibits the ability to be able to extract sufficient and relevant resilience data across the organisation.
>
> Confidence in data quality is also proving a challenge for organisations. Robust but transparent MI will provide visibility for the Board and Senior Managers to understand their end-to-end operational resilience environment and respond more quickly to threats and vulnerabilities.

What can be done?

It will be important as part of the mapping exercise to have a complete picture of all input and output data requirements along the end-to-end important business service chain and address material gaps in data quality.

A key success factor will be to understand the tooling environment and how best to optimise the tooling strategy that enables full reporting visibility for operational resilience.

Trend #6: Third Party risk management

> Most regulated firms will have complex third-party environments with multiple third parties, fourth parties and so on; as well as having invested heavily in recent years moving to cloud infrastructure.
>
> Therefore, it is critical that firms understand their exposure to third party risk as well as third party concentration risk regarding their Important Business Services but also generally as part of a well-planned Cloud and Cloud Exit strategy.
>
> The Final Policy and Supervisory Statements reiterate that Board and Senior Manager engagement is essential and that reliance on third parties and critical service providers must be fully understood. Notwithstanding the requirements within the UK to ensure adherence to the PRA’s ‘Outsourcing and Third-Party Risk Management’ Supervisory Statement SS2/21 under a Stressed Exit scenario; and within the EU to DORA’s strict requirements on third parties, which must all be collated in a register, and must be involved

in large-scale resilience testing.

What can be done?

Regulated firms need to prepare for March 2022 compliance with the PRA's expectations for outsourcing and third-party risk management right away by assessing gaps and defining clear milestone-driven action plans.

As a result of those new requirements, the visibility of outsourcing and third-party risk within the operational environment is much more critical. Firms will need to ensure that they have a complete and up to date inventory and that third party risks are fully documented and assessed together with exit planning and testing arrangements.

Mathew Wells is a Senior Manager and Operational Resilience expert at Wavestone

---

Article by MATHEW WELLS