SAI360

Risk | Learning | EHS | Sustainability

EBOOK

Leveraging technology in pursuit of operational resilience

The pressing need for operational resilience in the UK financial sector

The UK financial sector has encountered a host of exogenous shocks over the past two decades. Each event – from financial crises to geopolitical conflicts, a global pandemic – has presented institutions with new and dynamic challenges. At the same time, increased digitization has accelerated global interconnectedness, fostering a deep reliance on third parties and increasing the concentration of risk across the industry.

Most recently, concurrent global disruptions have forced financial institutions to double-down on resiliency planning, focusing on people, processes, technology and information as a means of managing the evolving threat landscape. The Covid-19 pandemic offers an example of the severe but plausible impacts of such circumstances – the necessity of hybrid work arrangements saw employees using less secure home setups with limited access controls and no endpoint protection. As a result, UK ransomware attacks doubled throughout 2021.[1]

Regulatory initiatives have evolved to mirror a common desire to cultivate a financial sector that is efficient, effective and resilient to all forms of disruption. While the recent pandemic thrust operational resilience back into the global media limelight, the Operational Resilience Framework began development far earlier off the back of a spate of major institutional outages from 2016-2018. Most notably, TSB's online payment services were disrupted for almost a week in April 2018, leaving customers unable to use online banking functionality.[2] Regulators across the UK have repeatedly reinforced that it is vital that banks provide reliable and resilient online services.

In this eBook, we will be taking a look at the key requirements of the Operational Resilience Framework, offering recommendations to institutions looking to enhance their resilience strategy. We will also explore the importance of leveraging technology within operational resiliency planning as a means of obtaining a competitive advantage.

1 https://www.rpc.co.uk/press-and-media/number-of-uk-ransomware-attacks-double-in-past-year/#:~:text=The%20number%20of%20ransomware%20attacks,RPC%2C%20the%20international%20law%20firm.

2 https://www.theregister.com/2018/04/23/tsb_systems_go_titsup_as_customers_cant_bank_online/

SECTION 1

Introducing the UK Financial regulators' Operational Resilience Framework

The Operational Resilience Framework was jointly developed by the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA), and the Bank of England in its capacity of supervising financial market infrastructures (FMIs), collectively 'the supervisory authorities'.[3] It was designed to enable British institutions to better prevent, adapt, respond to, recover and learn from operational disruptions. While financial institutions have always had requirements for disaster recovery and business continuity planning, this regulatory framing of the requirements by the regulators will force these firms to revisit and enhance those existing policies and disaster recovery provision.

The Operational Resilience framework sees the supervisory authorities adopting a proportionate and flexible approach in order to accommodate for the varied business models of UK financial institutions. Through improving banks' resilience, the regulators aim to minimize harm to consumers and protect market integrity.

The Operational Resilience Framework includes four main pillars;

3 https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf

1 – IDENTIFY IMPORTANT BUSINESS SERVICES

In terms of what constitutes "important business services," the regulators decided against prescribing a unified taxonomy, recognizing the fact that no two firms have exactly the same operational dependencies. Instead, the regulator provided two high-level principles to guide firms in their categorization. Important business services defined as those which, if disrupted, could;

a) Cause intolerable levels of harm to one or more of the firm's clients, or;

b) Pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.

Firms are required to review their important business services at least once per year, or whenever there is a material change to the business or the market in which it operates. In the Framework, "material change" includes:

a) The firm carrying out a new activity/ceasing to provide an existing activity

b) Outsourcing a new/existing service to a third-party service provider

c) Changes to an existing service in terms of scale or potential impact (e.g., number of customers)

2 – SET IMPACT TOLERANCES

The UK financial regulators consider firms are best placed to set their impact tolerances at the appropriate level in accordance with their risk appetite. This flexible approach is necessary given the wide range of firms in scope.[4] Firms should set impact tolerances at the point at which disruption could cause "intolerable harm" to end-customers or risk market integrity.

Institutions are encouraged to employ a breadth of metrics to measure impact tolerances, including the mandatory benchmark of duration/time. By using time as an indicator, regulators are encouraging firms to plan for time-critical threats where there could be limited time to react to disruption before intolerable harm or risk to market integrity is caused. Additionally, the use of time as a common metric provides a clear standard for incident response and enables inter-firm benchmarking.

Dual regulated firms[5] are required to set one impact tolerance at the first point at which there is an intolerable level of harm for the FCA's purposes. Under the Prudential Regulatory Authority's (PRA) rules, another separate tolerance is to be set at the point at which a firm's safety and soundness, or broader financial stability is at risk.

4 Banks, Building Societies, PRA-designated investment firms, PRA Solo Regulated Firms, Insurers, Recognized Investment Exchanges, Enhanced scope SM&CR firms, Entities authorized and registered under the Payment Services Regulations 2017 or Electronic Money Regulations 2011

5 In the context of UK financial services regulation, the term "dual regulation" refers to the split in regulatory responsibility for most regulated financial firms between two regulators: the PRA and the FCA.

3 – MAPPING AND SCENARIO TESTING

For firms to gain a complete view of their resilience, institutions must identify and document the people, processes, technology, facilities and information (resources) necessary to deliver each important business service.

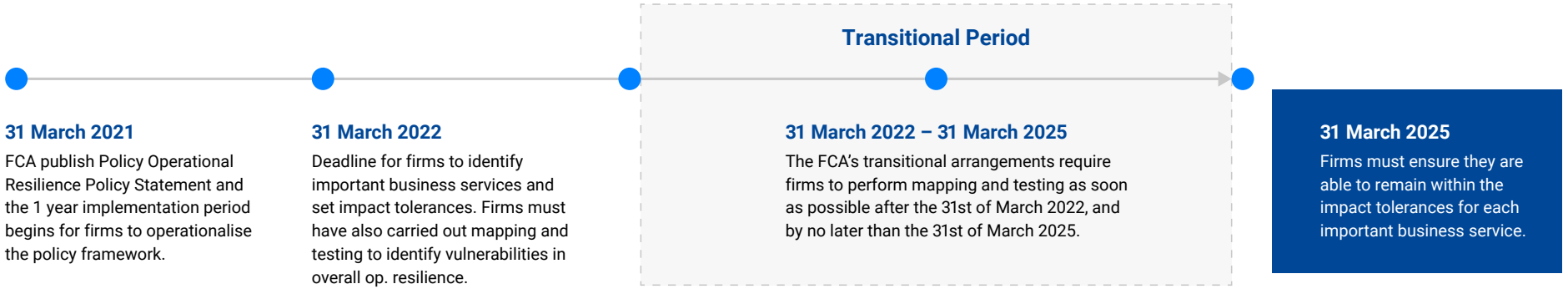
By the 31st of March 2022, institutions were required to carry out mapping to a level of sophistication required to identify important business services. Firms were also required to set impact tolerances and identify any vulnerabilities in their operational resilience. In-scope institutions now have until the 31st of March 2025, at the latest, to continue performing mapping with a view to remain within their designated impact tolerances.

4 – COMMUNICATIONS, GOVERNANCE AND SELF-ASSESSMENT:

Firms are required to design internal and external communication strategies to respond quickly and effectively to operational disruptions. Internal communication strategies should include escalation paths to manage communications during an incident and identify the appropriate decision makers. As part of their external communications strategy, firms should consider how they would provide important warnings or advice to consumers and other stakeholders, including where there is no direct line of communication.

Firms will need to compile self-assessment documentation highlighting *how* they meet their operational resilience requirements. This document should evidence the steps that the firm has taken to assess the impact of the regulatory policies, enhance frameworks, and embed the required methodologies to fulfil the operational resilience requirements. While institutions will not be required to submit the document to the FCA, it will need to be made available upon request.

A timeline of the FCA's Operational Resilience Framework



SECTION 2

Leveraging technology within your operational resilience strategy

1 – DEFINING YOUR KEY BUSINESS SERVICES

Considering the quantity of work that follows the identification of important business services, it is critical that firms get this step right. In identifying key business services, institutions are encouraged to prioritize those which deliver value to "external end-users." As a result, internal processes (such as payroll) do not meet the criteria.

For some firms, it may be beneficial to identify and document *all* business services before assessing which are to be classified as important, employing metrics such as the size and nature of the impacted consumer base. Regardless of the approach, organizations should identify each service as a separate function, so as to avoid conflating two services that, as per the rules, should be identified separately.

LEVERAGING TECHNOLOGY

A central theme underpinning a strong resilience strategy is evidence. Institutions must document the rationale for the classification of internal business services in order to justify decisions to internal and external stakeholders. Banks have traditionally been siloed organizations, with different departments using disparate systems for documentation. This inevitably limits scalability and causes immense challenges for institutions as they try to evidence decision making across multiple departments.

Technology such as SAI360's operational risk module offers risk consolidation techniques that allow banks to quickly summarize the risk profile of their important business services. By hosting this information in a centralized and accessible application, users can leverage instant data consolidation, documentation and disclosure to regulators and internal stakeholders.

2 – SETTING IMPACT TOLERANCES USING RISK METRICS

Once important business services have been identified, organizations must map impact tolerances in line with broader risk appetite. The FCA encourages firms to employ a breadth of quantifiable metrics to determine the maximum tolerable level of disruption, some of which may include:

- The number and types of consumers adversely affected
- The number of transactions affected
- The risk of financial loss to the firm where this could harm consumers
- Potential reputational damage where this could harm the firm's consumers

All impact tolerances should include the maximum level of tolerable *duration* of such a disruption. In doing so, firms are able to assess at what point disruption would pose a risk to financial stability or harm consumers.

A robust resilience strategy should prioritize mapping third-party dependencies in the provision of key business services, and firms will need to work closely with external providers to set and remain within designated impact tolerances. This is particularly important for ongoing compliance as remaining within the impact tolerances is the responsibility of the in-scope firm, irrespective of whether it uses third-parties.

LEVERAGING TECHNOLOGY

Manual approaches to setting impact analysis puts decision makers at risk of becoming overwhelmed by data in pursuit of the perfect answer. Available technology solutions allow firms to set impact tolerances based on quantifiable and configurable impact and likelihood models. This offers a foundation of information that is organized and sustainable, and which continuously evolves in line with changes to the firm's internal and external environments.

Third-party risk is notoriously difficult to monitor due to a lack of visibility into a firm's operations. Ultimately, it requires a degree of trust in an entity whose practices and processes cannot be controlled. Available software can ease the burden by enabling institutions to better detect vendor criticality through centralizing vendor records to generate risk profiles. Solutions, such as those offered by SAI360, facilitate ongoing third-party screening for an array of risks – including cyber, financial and credit risk – providing automated alerts to any changes in risk score.

3 – MAPPING DEPENDENCIES AND SCENARIO TESTING

The operations of incumbent financial institutions are particularly complex, with a heavy reliance on an array of technologies, siloed business divisions and an ecosystem of third and fourth parties. The FCA requires firms to develop value-stream (process and subprocess) maps in order to identify key dependencies. Scenario testing should then be utilized to highlight whether the institution has the necessary infrastructure in place to notify, route and escalate relevant parties for investigation should a disruption occur.

LEVERAGING TECHNOLOGY

Integrated technology offers a means of centralizing risk information, ensuring dependencies can be communicated and made visible to relevant stakeholders. Such solutions offer the capability to streamline action plans using automated and configurable workflows, assigning owners with triggers – emails, escalations, management sign-off and reports – to ensure investigation and root cause analysis is effective across any scenario.

SAI360's Operational Risk Module continuously monitors risks by leveraging key risk indicators (KRIs), enabling firms to define thresholds that trigger response actions and recognise trends across KRIs.

4 – DEVELOPING YOUR INTERNAL AND EXTERNAL COMMUNICATION PLANS

Bank's board of directors may not necessarily be experts in operational risk management, so firms must ensure they are armed with sufficient data and intelligence to make informed decisions. Risk metrics can be difficult to interpret, however, some institutions need to provide visible and actionable reports with an aggregated view of real-time risk metrics. The wider stakeholder group must also be sufficiently informed in order to react appropriately to disruptions. In the event that a disruption does occur, speed is paramount, and information must be disseminated quickly to relevant response teams.

As previously mentioned, firms must compile self-assessment documentation detailing and justifying the approaches and methodologies used across their entire resilience strategy.

LEVERAGING TECHNOLOGY

Centralized data aggregation facilitates the creation of customized charts and recurring status and regulatory reports in one system. Configurable dashboards and actionable analytics can be generated to provide digestible strategic insights to senior leadership through providing heat maps and risk trends with overviews and relevant details. Broader internal communication can be streamlined with integrated mass notification systems, delivering automated alerts to relevant departments to accelerate incident response.

Institutions should also leverage technology to support self-assessment documentation. Solutions such as SAI360's Operational Risk Module provide top-down and bottom-up assessments with consolidation techniques to summarize the risk profile for a business unit or the organization as a whole. Moreover, the software offers a full audit trail enabling stakeholders to evidence and justify the methodologies deployed within the broader resilience strategy.

SECTION 3

Operational Resilience: a new source of competitive advantage?

Operational resilience reduces the potential impact of disruptions by enabling companies to anticipate, prepare for and respond to shocks. Customers, stakeholders, investors and regulators value resilience and reliability in the firms they engage with. If institutions can reinforce resilience as a core brand principle and evidence its application, it can offer a competitive advantage by improving customer retention, operational efficiency and increasing investor confidence.

Customer trust is difficult to earn, but easy to lose. Modern technology has led customers to expect seamless customer service and 24/7 accessibility, many are quick to criticize, or worse, change providers should they be dissatisfied. Firms are required to manage these expectations whilst constantly innovating their product and service offerings to remain competitive. Customer service and innovation i s enabled by employees and IT infrastructure. Resilience enhances employee security and improves retention and attraction. Resilience also fosters more stable and reliable IT infrastructure, allowing firms and their employees to focus on value-added services, rather than constant fixes, security issues and remediation.

Brand reputation, the credibility of a firm and its leadership team are directly enhanced by resilience. Shareholders seek out resilient organizations in an attempt to drive returns, with the most operationally resilient firms likely to be the most efficient and economical, with a positive impact on risk adequacy, customer agility, all of which directly impact top line growth.

TECHNOLOGY, REAP THE REWARDS IN RECORD TIME

The challenges of implementing procedures in line with new resiliency requirements have been made clear by in-scope firms, with many fearful that rigorous mapping and scenario testing will impact business-as-usual operations. The FCA recognizes the added burden on institutions and strongly advises “necessary investments” to enable them to operate consistently within their impact tolerances.

It is critical that firms explore opportunities to leverage technology where possible to best minimize disruption to other activities while meeting regulatory requirements. Solutions, such as those offered by SAI360, facilitate enhanced productivity through increasing automation and accessibility while fostering more effective risk identification and mitigation. Utilizing technology also simplifies risk analysis, reduces human error and reduces regulatory risk through effective reporting.

SEE WHAT SAI360 HAS TO OFFER

SAI360 are GRC experts and a leading cloud-based operational resilience and business continuity management solution provider. Our modular approach allows you to take advantage of configurable solutions and quickly shape them to help you thrive in the evolving Governance, Risk and Compliance landscape.

To learn more about the SAI360 platform and how we can advance your GRC goals, contact us online to set up a call with one of our representatives.

SAI360

Risk | Learning | EHS | Sustainability

ABOUT SAI360

SAI360 is a leading provider of Risk, Learning, EHS, and Sustainability software. Our cloud-first SAI360 platform contains flexible, scalable, and configurable modules for a better vantage point on risk management. Our unified approach to risk management is what sets us apart, helping organizations across the globe manage risk, create trust, and achieve business resilience for over 25 years.

SAI360 is headquartered in Chicago, U.S., and operates across Europe, the Middle East, Africa, the Americas, Asia, and the Pacific. Discover more at **sai360.com/health** or follow us on **LinkedIn**. To see our platform in action, **request a demo**.

93106 0822