KPMG

Operational Resilience in Financial Services

Since the global financial crisis in 2008, industry leaders and supervisory authorities alike have placed a strong focus on financial services organisation's ability to demonstrate resilience. Although the outcome of the Covid-19 pandemic stress testing of global financial institutions indicated that the industry remained resilient, one of the top supervisory priorities for financial services regulators worldwide continues to be **Operational Resilience** and it is expected to be a key regulatory focus area over the coming years.

What is Operational Resilience?

Operational resilience is defined as the capacity of a financial services organisation to anticipate, prepare, respond, adapt, recover and learn from business disruption.

Why is Operational Resilience important?

The requirement for financial services organisations to rapidly identify and mitigate constantly evolving operational risks has intensified as a result of the ongoing effects of the pandemic, severe supply chain problems brought on by the geopolitical crisis, an unprecedented rise in commodity prices, and significant fluctuations in currency values supplemented by the ongoing escalated stages of loadshedding. This is a chance to create a strong framework that is appropriately tested for a range of stresses and is fully integrated into the organisation's risk management procedures rather than merely a regulatory requirement that must be evaluated and approved on a yearly basis.

The South African Reserve Bank Prudential Authority:

The South African Reserve Bank published a directive on operational resilience in September 2021, instructing South African banks to assess the adequacy and robustness of their current business procedures, policies, and practices in adhering to the operational resilience principles established by the Basel Committee on Banking Supervision (BCBS).

The Prudential Authority ("PA") has further determined that the flavour-of-the-year for 2023 is organisational resilience and climate related risks. The chairperson of the organisation's board is therefore now required to present on various aspects of the firm's organisational resilience strategy and implementation to the PA.

Regulations around the world

From a global perspective, the Basel Committee on Banking Supervision issued the Principles for Operational Resilience in March 2021, in an effort to assist organisations in implementing an effective operational resilience programme. Regulators across the world have noted an increased reliance on technology from organisations in the financial services sector as an emerging risk as any disruption to this technology could have serious repercussions from an operational resilience programme perspective.

The following areas of concern have been noted from a global perspective:

- Poor governance and oversight of outsourced functions and third-party service providers;
- Insufficient resilient legacy IT systems with poor cyber security; and
- Lack of contingency plans for business disruptions.

Basel Committee on Banking Supervision Principles of Operational Resilience

How financial services firms can develop an effective operational resilience framework

Although the majority of banks and insurers in South Africa are still in the early phases of establishing and/or strengthening their operational resilience frameworks, new regulations have supported the rise of operational resilience programmes within the financial services sector. The following are key actions that should be considered when developing, reviewing and / updating an operational resilience framework:

- **Important Business Services (IBS)**: The starting point is critical in determining how operational resilience will be designed. This is explicitly defined by regulators as a business service delivered to an external end-user.
- **Mapping**: The identification and documenting of resources required to deliver and support activities within IBS.
- **Impact Tolerances**: This determines the acceptable level of disruption to an Important Business Service, as measured by the maximum acceptable duration and the extent of the interruption.
- **Scenario testing**: Testing the ability to withstand a severe disruptive event with reference to impact tolerance and identify resilience gaps from the validation exercise.
- **Governance and Leadership**: The Board is expected to supervise and approve all operational resilience components, as well as seek assurance that appropriate strategies, procedures, and systems are in place to identify IBS, define impact tolerances, map resources required, and test the response and recovery procedures.
- **Communication**: The development of communication plans to be triggered when services are disrupted.
- **Self-Assessment**: Documentation of a self assessment report, on measuring of compliance with operational resilience regulations, methodology applied, vulnerabilities, scenario testing, and remedial actions noted.

Impact of inadequate operational Resilience?

A key message from an operational resilience forum held in London by the Financial Conduct Authority noted that “Operational resilience is about preventing operational incidents from impacting consumers, financial markets and financial system.”

Inadequate operational resilience may hinder access to financial services and products and raise broader questions about the dependability of financial institutions and the financial system integrity, which may have a detrimental effect on financial inclusion.

Organisations may incur significant costs as a result of not operating during a period of disruption. They can suffer not only financial, but reputational and operational damage which could ultimately threaten the organisation’s overall viability and have negative economic impact. Furthermore, the economic impact of such an event would be immense, potentially resulting in job losses, loss of production and data, civil unrest, loss of communications and further strain on the economy.

Organisations may also face consequences of non-compliance to legal and regulatory requirements.

Turning operational resilience into a business opportunity?

- Generate synergies across strategic, financial and operational resilience.
- Enhance customer trust and loyalty.
- Reduce operational risks and costs of disruption.
- Enhance positioning for mergers, acquisitions and moves into new areas of business or new ways of doing business.
- Allocate resources more effectively and efficiently.
- Ensures regulatory compliance while establishing a strategic value.

Energy crisis through operational resilience planning:

A pertinent risk, organisations should be considering as a starting point to improving operational resilience, is the potential collapse of the national power grid in South Africa. With escalated stages of loadshedding, ageing infrastructure and the lack of routine maintenance, organisations should consider the impact of provincial blackouts which may arise and/or extensive power outages which could lead to an unprecedented national grid failure. Whether it materialises or not, there is benefit in preparing for the outcome as we have seen numerous black swan events materialise in recent years. The country's power supply has already been in a state of crisis, with load shedding and power outages becoming increasingly frequent. A collapse of the national power grid could be catastrophic, causing widespread disruption to businesses and households.

Contact us

Nashikta Angadh (AMBCI)
National Business Resilience Lead Partner
President: BCI Southern African Chapter
KPMG South Africa
nashikta.angadh@kpmg.co.za
+27 82 719 1368

Sabelo Nsiba (CISA, Cobit, Cyber Security)
National Business Resilience Manager
KPMG South Africa
sabelo.nsiba@kpmg.co.za
+27 72 376 9632

Michelle Dubois
Africa Regulatory Centre of Excellence Lead
KPMG South Africa
michelle.dubois@kpmg.co.za
+27 60 997 4512

kpmg.com/socialmedia