Michelle Dubois

Senior Manager
Regulatory Centre of Excellence lead
Tel: +27 60 997 4512
Email: michelle.dubois@kpmg.co.za

Anticipate, adapt and thrive... operational resilience for insurers

What is operational resilience?

Operational resilience is well embedded in the banking sector. The Basel Committee on Banking Supervision (BCBS) defines operational resilience as "the ability of a bank to deliver critical operations during disruption"[1]. They stated further that this ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption.

In a letter to all significant institutions in 2020, the European Central Bank (ECB) commented that supervised entities are expected to review their business continuity plans and consider what actions can be taken to enhance preparedness to minimise the potential adverse effects of the spread of COVID-19. In particular, banks could be challenged on their operational capabilities in affected areas including constraints of key third party outsourced service providers and suppliers to maintain critical processes.

In South Africa the Prudential Authority (PA) released a guidance note in April 2023. This directive requires banks to "consider the adequacy and robustness of the banks' current policies, processes and practices related to operational resilience, against the best practices contained in the BCBS paper on principles for operational resilience".

So where does that leave insurers?

There is currently no formal directive for the non-banking financial sector. However, in Communication 1 of 2023, the PA has specifically drawn insurers into the discussion with the flavour of the year topic, organisational resilience, being applied to both banking and insurance entities. This leaves us in no doubt as to the significance of operational resilience for insurers and clearly outlines the regulator's expectations.

In the flavour of the year, the PA refers to organisational resilience and defines this as the ability of the organisation to absorb and adapt in a changing environment to enable it to deliver on its objectives as well as to survive and prosper.

The shift from business continuity

Is operational resilience simply an evolution of business continuity management? The PA has made it clear that operational resilience is not business continuity on steroids.

The simplest distinction between the two is the fact that business continuity management is a reactive response to an incident, whereas operational resilience is proactive.

[1] Basel Committee on Banking Supervision issued principles for operational resilience and risk in a media release 31 March 2021.

A well thought out operational resilience plan is an assessment of the business environment, allowing the organisation to implement procedures and mitigation strategies across the business ecosystem before the occurrence of a disruptive event.

Operational resilience casts a wider net, taking cognisance of business continuity plans, cyber risk policies, facilities and operations and forces organisations to consider the broader impact of disruption, including the contagion of events. However, at the forefront is the ability of the organisation to deliver to customers in the face of business disruption.

Organisational resilience focuses on the ability of an organisation to continue providing critical services and operations during and after a disruption and is a broader concept that encompasses the ability of an organisation to adapt and thrive in the face of change, uncertainty and disruption. COVID-19 changed the way we look at continuity planning and crisis management and extended this concept further to organisational resilience.

Disruption facing insurers

In order to prepare for disruption, insurers need to critically assess their business operations. In the last few years, the sector has been preoccupied with the effects of the COVID-19 pandemic. The transition to remote working and the consequent risk to health dominated the continuity agenda. Insurers were suddenly faced with a steep increase in claims on certain product lines such as business interruption, retrenchment cover, life cover, funeral cover and income protection. While the immediate financial implications meant that profits took a hit, insurers held fast with reserves enabling most insurers to pay claims as their products had promised. In the meantime, product development teams started to assess which products would remain viable for new business and which would need to be altered or done away with completely.

Some product lines were hit harder than others. After stranded travellers were repatriated, there was a ban on travel which meant a complete shutdown for all travel insurance sales, whilst claims for cancelled trips soared. Distribution models dependant on medical underwriting stagnated as clients were not willing or able to visit labs and doctors for screening. As businesses locked down and retrenchments were announced, customers turned to their credit life policies for assistance in settling debt. At the same time new credit applications were paused as customers faced economic uncertainty and the banks increased lending criteria. Logistically, claims processes became complicated.

Insurers needed to adapt quickly in order to protect their essential business services. Risk management strategies were applied to assess and address pandemic-related risks in addition to using various methods to assess claims, evaluate policies and determine pricing models that were based on a changing risk landscape. Insurers amended processes to expand telephonic underwriting services, enable policyholders to submit documents with electronic signatures or app-based claims. Furthermore, product offerings became more flexible to accommodate customers with many insurers offering premium holidays.

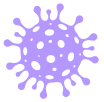
Remote work was essential to ensure insurers could provide ongoing service delivery. This meant that previously office bound employees needed to be provided with laptop computers and cell phones. Investment in connectivity and bandwidth was essential to enable this new world of work. When lockdown eased and certain services could resume, some business areas returned to the premises to work in shifts, reducing the number of people in the office at any one time to an acceptable COVID-19 preventing ratio. Life insurers sent nurses out to clients to conduct basic medical examinations for underwriting and claims assessors used drones and social media to aid in their investigations.

Looking ahead, insurers should prioritise identifying critical services, defining impact tolerances and conducting rigorous scenario-based exercises to determine their readiness in the face of disruptions. A key element to consider is horizon scanning to ensure that risks, threats and opportunities are identified in a timely manner for immediate visibility and corrective action.

The Business Continuity Institute has identified the following factors as part of its risk and threat assessment for the next five years:

Cyber attack and data breach

Non-occupational disease



Climate risk

Technology/telecoms failure

Talent concerns

Climate risk has resurfaced as a key area of focus with recent weather patterns such as the Kwa-Zulu Natal floods and Johannesburg earthquake escalating sustainability concerns. Other threats on the horizon include loss of communications, cyber breaches and prolonged power outages and water supply disruptions. How will your business operate if your communications network goes down because of a flood? Do you need to invest in satellite phones for executive members and key personnel? Are your physical premises secure in the event of civil unrest? Do you have back up power for an extended outage where fuel supplies for generators run dry? Do you have a view of your key employees' succession plan as loss of talent due to emigration and semi-emigration is something that insurers are grappling with. These questions and more are all a critical part of your operational resilience plan.

Survival of the fittest

One of the first steps in ensuring operational resilience is integrating operational resilience into the insurer's strategy. Resilience by design will ensure that there is agility in the strategy to adapt to disruption without compromising the insurer's strategic objectives. It is critical to build awareness around the concept of resilience, integrating this into the culture of the organisation so that it is a constant consideration in decision making. First prize is to embed operational resilience thinking into business as usual where "resilience in everything we do", becomes the mantra.

Assigning responsibility within the organisation is important. The role needs to be one that is of strategic importance with sufficient seniority to give it the focus and attention it requires. Ultimately allocating someone to lead the charge is critical, but that person needs to have the support of the collective. The best way to achieve this is to make sure that the executive is accountable with operational resilience part of their performance measures.

Anticipate, adapt and thrive

The PA's flavour of the year requires organisations to consider some of the pertinent risks facing the sector and to present the organisational strategy to the regulator on the following six areas:

- **Governance and leadership**
  The regulator is looking for insurers to demonstrate how they have defined organisational resilience and adopted this definition to strengthen the culture of the organisation. The flavour of the year clearly advises insurers that they need to present their strategy for operation in the event of disruption as well as clearly articulate the role of oversight and assurance providers in the organisational resilience process.

- **Risk management**
  This requirement focuses on the insurer's risk management process and how the insurer identifies and assesses threats and risks, how the insurer monitors and responds to them and how these are reported and escalated.

- **Mapping of interconnections and interdependencies**
  Once the insurer's critical operations have been identified, the PA requires that they illustrate how these are interconnected and interdependent (both internal and external, local, regional and internationally).

- **Change readiness**
  The regulator would like to see how insurers are embracing agility and a change mindset so that products can be adapted to fit an environment that is constantly changing.

- **Situational awareness**
  In order to meet this requirement, the insurer must evidence how they have a process to test its resilience against various disruptions and how they have learnt from previous crises.

- **Information and communications technology, including cybersecurity**
  The insurer must demonstrate that it has a process and defined framework to protect its information and communications technology and infrastructure and a plan to protect itself against cyber attacks.

Third party dependency and supply chain

In order for insurers to gain comfort that they are resilient in the event of a risk or threat manifesting, they must satisfy themselves that their third-party providers and outsourced suppliers have the same resilience measures in place.

In our discussions with the regulator, it was clear that they are looking to see documented and tested operational resilience plans. For insurance companies these range from the expansion of existing and traditional risk management levers like reinsurance and detailed risk management of outsourced service providers, all the way down to physical remediation plans like where everyone will work if the building burns down or what will happen if the national power grid fails for a week. Implementing these solutions depends on the needs and risks facing each organisation. This in turn is driven by the products insurers sell – life insurance companies have very different concerns to non-life insurers. Life insurers may find their ability to make life-saving claim payments very difficult if the banking system fails; non-life insurers may find it difficult to have vehicles repaired if the repairers they have outsourced arrangements with are unable to work because essential imported panel beating equipment cannot be delivered from Durban harbour to Johannesburg.

> The bottom line is that the pursuit of operational resilience is not local and regulatory, it is strategic and global.

The Business Continuity Institute Operational Resilience Survey 2023 for the Africa Region found that the main reasons that organisations are incorporating operational resilience programmes are because of regulatory requirements and 73% of them wish to align to good practices. The Financial Sector Conduct Authority has expressed that crisis is the new normal, which means that operational resilience is far from a regulatory compliance matter and should rather be viewed as a strategic stepping-stone for insurers to not only survive but thrive.