Navigating Operational Resilience in the Insurance Industry

September 2023

Operational Resilience emerged as a key agenda item for insurers as they responded to the challenges posed by the Covid-19 pandemic. This was not just due to increasing regulatory scrutiny, but also as a means for them to demonstrate their commitment to safeguarding customer assets and maintaining service availability throughout business disruptions.

Insurers in Hong Kong (SAR) are relatively new to this topic. Due to regulatory requirements, banks have already started their operational resilience implementation journey. While insurers traditionally maintain a recovery / resolution plan and Business Continuity Plan, operational resilience goes beyond these by taking a customer-centric approach, with the objective to avoid causing intolerable harm to customers or impacting the firm's long-term viability.

Forward-thinking insurance firms are leveraging operational resilience as a strategic differentiator to stand out and gain competitive advantage in the industry. This presents an opportunity for insurers in Hong Kong to build end-to-end operational processes to serve their customers through disruption and to focus on prioritisation of services. Insurers can incorporate better operational resilience practice to align cyber resilience, third-party outsourcing and business continuity management.

KPMG has been supporting our clients to design and implement Operational Resilience (OR) frameworks in different jurisdictions with our Powered Resilience Solution, which is based on the successful delivery of OR frameworks to our clients, various regulatory insights and market leading practices.

What is Operational Resilience?

The International Association of Insurance Supervisors (IAIS)[1] has published an Issues Paper on Insurance Sector Operational Resilience, which defines an operationally resilient insurer as below:

Definition of Operational Resilience

> "An operationally resilient insurer is one that can encounter, withstand, mitigate, recover and learn from the impact of a broad range of events that have the potential to disrupt the normal course of business by impacting critical operations or systems. Operational resilience rests upon the assumption that disruptions will occur and that insurers should consider their tolerance for such disruptions and take this into account when devising their operational framework."

Key areas to consider when building an Operational Resilience framework

Referring to the IAIS Paper, insurers (including both insurance groups and local insurers in Hong Kong) can consider the following four key areas when building their Operational Resilience Framework as they start to prepare to manage all risks that have the potential to affect critical operations delivery.

Board and Senior Management Responsibility

The Board is ultimately responsible for overseeing a robust Operational Resilience Framework, while senior management should account for effective design and implementation of the framework.

IT Third-party Outsourcing

Although IT third-party outsourcing has improved operational resilience, the concentration risk from outsourcing critical IT services to one or a few providers should be properly managed.

Cyber Resilience

It is fundamental for insurance companies to put in place a sound cyber resilience framework that can withstand and react to increasing cyber risks, and ensure the framework is effective through regular assessment.

Business Continuity Management

With increasing operational disruptions, insurers should proactively adapt to the evolving risk landscape by integrating Business Continuity Management across business functions.

As at time of publication, the Hong Kong Insurance Authority (HKIA) had not yet issued a specific operational resilience guideline. However, the abovementioned areas have been covered across various existing guidelines – such as Guideline 10, 14, 20, 21 and 32[2].

Note 1: Established in 1994, the IAIS is a voluntary membership organization of insurance supervisors and regulators from more than 200 jurisdictions.
Note 2: GL10, GL14, GL20, GL21 and GL32 refer to the Guideline on The Corporate Governance of Authorized Insurers, the Guideline on Outsourcing, the Guideline on Cybersecurity, the Guideline on Enterprise Risk Management and the Guideline on Group Supervision respectively.

Board and senior management responsibility

An insurer's Board is ultimately responsible for overseeing the establishment of a robust governance framework. Insurers with a strong and effective governance framework are better placed to prevent, adapt and respond to operational disruptions.

Senior management (Design and implementation)	The Board / Board-level committee (Oversight)
Develop OR framework and update it regularly	Review and approve OR framework
Ensure sufficient resources allocation	Possess adequate knowledge, skills and experience
Implement and report regularly to the Board	Oversee implementation and effective communication
Set up remediation plans to address deficiencies	Ensure priority of remedial actions

Cyber resilience

The insurance sector relies heavily on digital technologies, intensifying the need for a robust cyber resilience framework that can withstand and respond to increasing cyber risks. Key challenges are summarised below:

There is a need to enhance the skillset (especially in areas such as data and AI) to manage cyber security. As cyber attacks have become more advanced, insurers may need to upgrade their cyber resilience framework as well as the expertise to manage it.

Cyber resilience require proactively managing risks. Insurers can leverage the use of a single source of data to build risk indicators to better inform and manage cyber and operational resiliency.

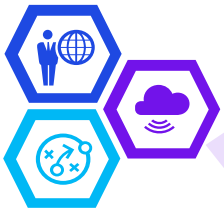
Accurate data and tooling platforms will be needed to support group or local business functions for change management, managing risks to identify potential vulnerabilities and to follow up on remedial actions. These platforms act as the repository of OR data and information, such as the list of OR parameters, mapping documentation and audit trail.

IT third-party outsourcing

The insurance sector's response to the Covid-19 pandemic demonstrates how third-party service providers and outsourced providers can contribute to the improved resilience of institutions. However, an overreliance on IT third-party outsourcing comes with increased operational risks and challenges. Some of the challenges and risks include:

For larger insurance groups, multiple entities or functions may be dependent on services provided by the same, or a few, internal or external service providers.

An increase in the use of non-regulated subcontractors and a growing dependence on complex supply chains to deliver critical IT services has the potential to increase compliance risk.



Insurers may have limited capability to address the nature of concentration risk in isolation. For example, a disruption in the use of the cloud could result in wider system disruptions across the industry.

Intra-group and other group relationships are critical, where local business that are reliant on the intra-group services using a common data platform, data services or system application services provided by the group.

Business Continuity Management

Given the interconnections and interdependencies as well as the complex functioning of the insurance sector, it is imperative that insurers adopt sound and prudent management practices to ensure business continuity in the event of an operational incident. Key challenges that insurers are facing include:

With increased operational disruptions, there is a need to integrate Business Continuity Management practices into other relevant operational risk management processes, with consideration of critical operations[3] and all key internal / external dependencies (such as a third party's Business Continuity Plans).

Business Continuity Management scope should be extended to encompass a wider range of events and business operations, such as failure of material outsourcing services, IT infrastructure failure and large-scale cyber attacks.

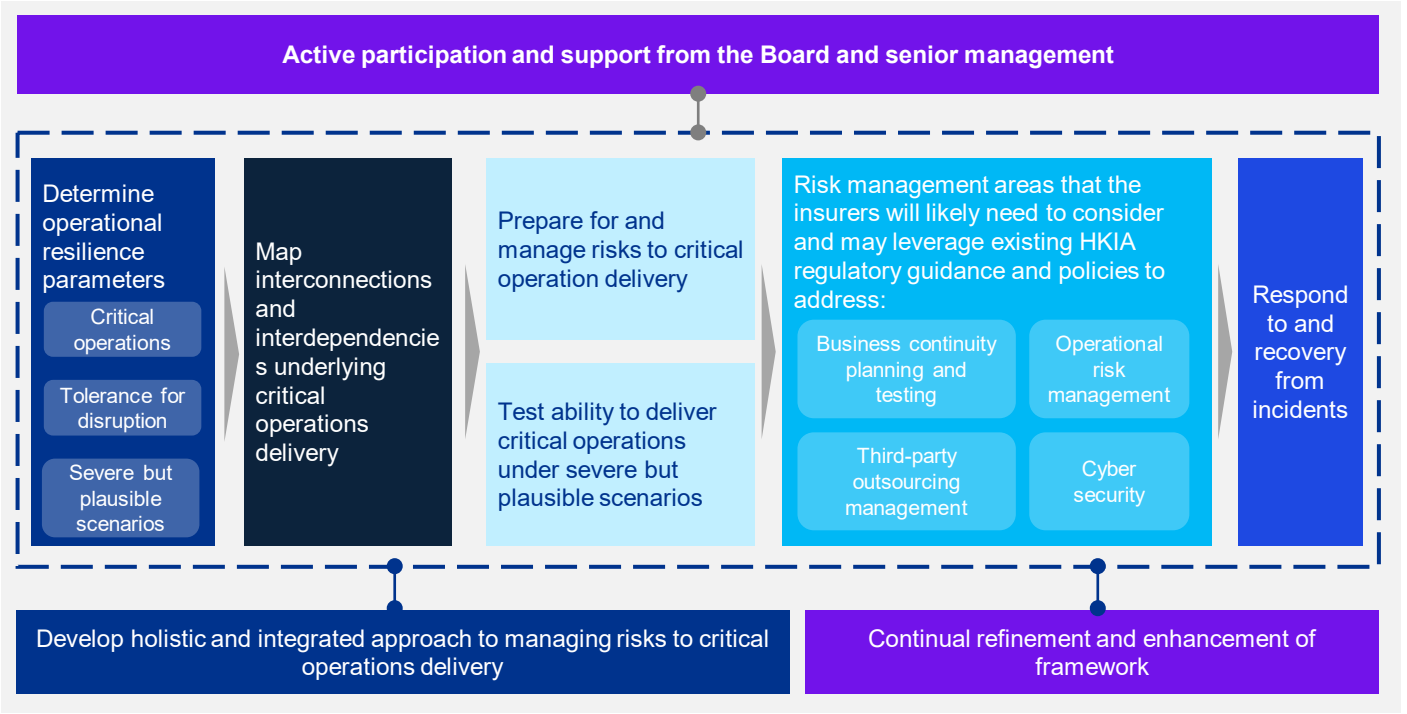
Before the Covid-19 pandemic, business continuity strategies focused on addressing short-term impact scenarios. Insurers should assess whether their Business Continuity Plans are forward-looking and remain fit for purpose, or if revisions to policies and procedures are required.

Note 3: The number of critical operations identified should be commensurate with the size, nature and complexity of the insurers operations. A typical example of critical operation for an insurer is claims management.

KPMG's approach to developing a holistic Operational Resilience framework

An insurer's Board is ultimately responsible for overseeing the establishment of a robust governance framework with clear roles and responsibilities to manage operational disruptions. Meanwhile, to develop and implement an operational resilience framework requires sufficient resources (financial and non-financial). Forward-thinking organizations should consider leveraging operational resilience as a differentiating factor in the market, thereby driving insurance industry-leading practices rather than just a regulatory compliance exercise.

KPMG's Powered Resilience Solution has helped financial institutions across the globe accelerate the development of a holistic Operational Resilience framework.



How can we support your Operational Resilience journey?

If you would like to know more about Operational Resilience and how KPMG can support you on operational resilience planning and implementation, below are a few areas for consideration on ways to get started on your OR journey.

Gap analysis of the insurer's current state compared to the HKIA's existing regulatory expectations; develop **high level implementation plan** or **roadmap**

Enhancement of the insurer's **existing incident management programme** to effectively respond to and manage disruptions

Operating model design embedding operational resilience with considerations given to embedding resilience within the insurer's core business processes, people and governance

Share industry best practices for Operational Risk Management and Business Continuity Planning

Identify operational resilience parameters identification, such as critical operations, tolerance for disruption and severe but plausible scenarios

Scenario testing exercise for critical operations including testing design, execution and preparation for formal testing report

Vulnerability assessment to identify and document the insurer's vulnerabilities and potential risks underlying critical operation delivery (eg people, technology, information and facilities)

KPMG has a global, multi-disciplinary team with subject matter advisors who have significant experience and capability across Operational Resilience, Operational Risk, Business Continuity Plan / Business Continuity Management, Recovery and Resolution Planning, and Cyber and Technology. We can draw on this depth of expertise to ensure that our clients have access to the right perspectives as we collaborate on an Operational Resilience Programme that meets your needs.

Contact us

If you would like to further discuss Operational Resilience in the insurance sector, please contact us:

Erik Bleekrode
Head of Insurance, Asia Pacific / Co-Head of Insurance, China
KPMG China
T: +852 2826 7218
E: erik.bleekrode@kpmg.com

Walkman Lee
Co-Head of Insurance, China
KPMG China
T. +86 8508 7043
E. walkman.lee@kpmg.com

Abhishek Kumar
Partner, Co-Head, Financial Services Risk Consulting, Hong Kong (SAR)
KPMG China
T: +852 2847 5120
E: abhishek.kumar@kpmg.com

Cara Moey
Director, Operational Resilience Solution Lead, Hong Kong (SAR)
KPMG China
T. +852 3927 4652
E. cara.moey@kpmg.com

Lanis Lam
Partner, Technology Resilience Solution Lead, Hong Kong (SAR)
KPMG China
T. +852 2143 8803
E. lanis.lam@kpmg.com

Bhagya Perera
Director, Cyber Resilience Solution Lead, Hong Kong (SAR)
KPMG China
T. +852 2685 7321
E. bhagya.perera@kpmg.com

Kris Pearson
Associate Director, Hong Kong (SAR)
KPMG China
T. +852 2685 7737
E. kris.pearson@kpmg.com

Daisy Jiao
Regulatory Affairs Expert, Hong Kong (SAR)
KPMG China
T. +852 2826 7134
E. daisy.jiao@kpmg.com

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg/cn/en/home/about/offices.html

kpmg.com/cn/socialmedia