Aurexia

ASIA PACIFIC REGULATORY WATCH

Revised outsourcing-related requirements and expectations for banks in Singapore

Implementation of Operational Resilience Standards in Hong Kong: learnings from BCBS' adoption assessment

RegTech Corner – Kaiko

Aurexia Institute

Asia Pacific Edition, March 2024

Foreword

We are delighted to publish the latest issue of Aurexia's Asia Pacific Regulatory Watch, our quarterly publication on regulatory developments and their impact on banks, asset and wealth managers, insurers and the wider financial services industry in the region.

In this RegWatch APAC issue, we are discussing the following topics:

- **Revised MAS expectations for outsourcing management its Notice 658 and Guidelines**

  In December 2023, MAS issued revised requirements and expectations and introduced a new classification scheme for outsourcing services. This impacts banks on several layers including risk assessment of providers, outsourcing agreement terms, as well as monitoring and reporting.

- **Operational Resilience – learnings from BCBS' adoption assessment for banks in Hong Kong**

  As banks in Hong Kong move to implement HKMA's SPM OR-2 on Operational Resilience, BCBS' assessment of the adoption of its 'Principles for Operational Resilience' provides valuable lessons and best practices from around the globe. In this article, we explore how Hong Kong-based banks can leverage and reflect these insights in implementing their Operational Resilience framework.

We trust you will find our articles informative and insightful. Should you wish to delve deeper into any of the topics discussed or share your thoughts, please feel free to reach out.

Enjoy reading this issue of our RegWatch APAC!

Sithi SIRIMANOTHAM
Partner & Group COO

Sebastian L SOHN
Director (Singapore)

Contents

Revised outsourcing-related requirements and expectations for banks in Singapore

Leveraging on external providers and outsourcing has become common practice among banks and financial institutions – driven by potential efficiency gains, scalability, expertise, and the ability to focus on core competencies.

However, this practice comes with certain risks outside of banks' immediate control. This was highlighted in October 2023 when two bank's faced significant system outages and service disruptions due to cooling issues in a service provider's data centre. If not monitored correctly, outsourcing can have adverse effects and undermine the bank's value chain. The risks related to outsourcing can have material impact on the 'business, the customers, the ability of the bank to manage its risks and to comply with laws and regulation' (MAS Notice 658).

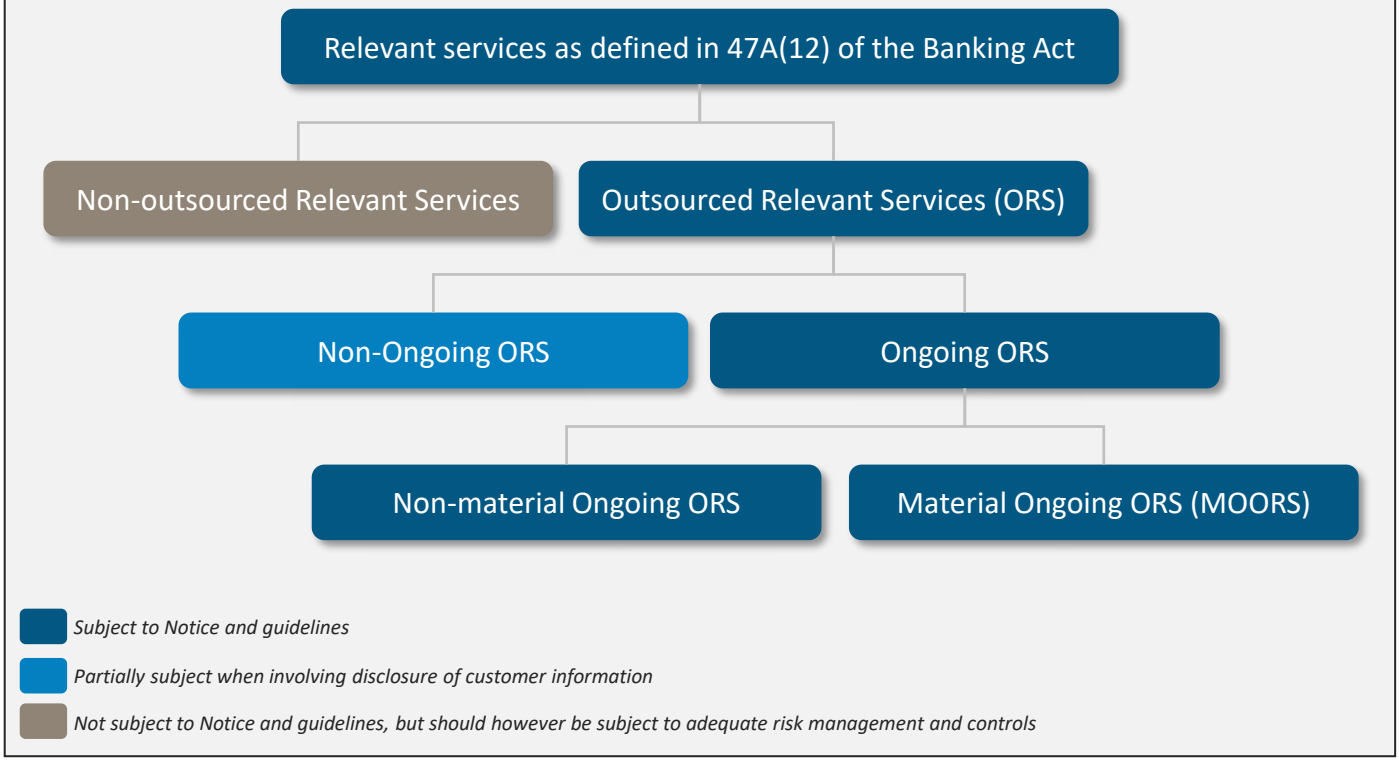
In December 2023, the MAS released a new Outsourcing Notice for banks (Notice 658) under the Banking Act 1970, setting out operational and risk management requirements for outsourced relevant services. The requirements, incorporated in the new Outsourcing Guidelines for banks add additional scrutiny expected from banks with more reporting and disclosure requirements. Both, the Notice and the Guidelines will become effective on 11th December 2024.

To guide banks in identifying the categories applicable to the respective outsourcing service, MAS provided four appendices in the notice, listing:

- relevant services integral to any business hat the bank may carry on under section 30.1 of the Act,
- relevant services excluded from the definition of 'outsourced relevant services,
- relevant services considered as **outsourced relevant services**,
- exempted outsourced relevant services.

This article explores the changes introduced by MAS Notice 658 and the implications for banks in Singapore. Requirements on notably materiality assessment and senior management / board governance are included in the guidelines on outsourcing for banks.

Classification of outsourced services



Source: MAS outsourcing guidelines for Banks – Annex 3

Regulatory requirements for different types of outsourcing activities

In the Notice 658 banks, MAS focuses on specific outsourcing services and draws a clear distinction between:

- **outsourced relevant services (ORS)**, defined as services usually performed by the bank and integral to any business the bank may carry on,
- **material ongoing outsourced relevant services** (MOORS) defined as ongoing outsourced relevant services that can materially affect the business of the bank and the customer, and
- all outsourced relevant services that include **disclosure of customer information** which refers to data relating to an account of a customer or a deposit information.

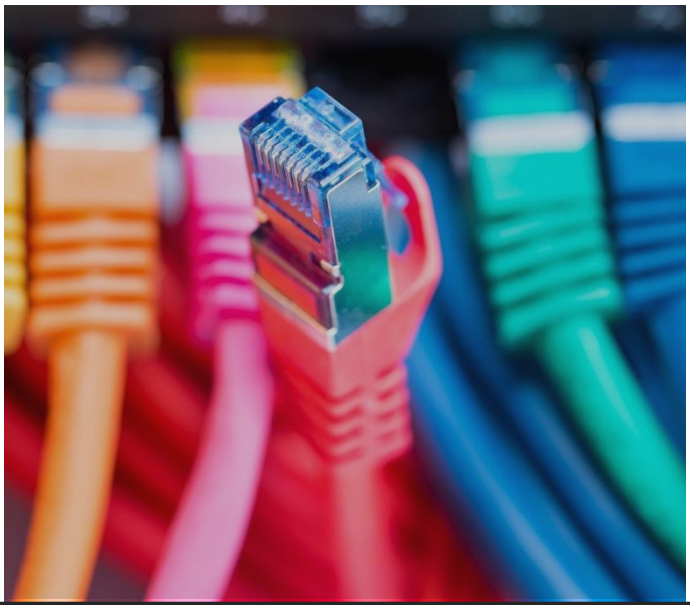
I - Outsourced relevant services

a. Outsourcing register

MAS expands the maintenance and reporting requirements for a register on outsourced relevant services and provides a revised, more comprehensive outsourcing register template. Banks need to periodically update the register and submit it semi-annually to the authority.

b. Group policy

All banks incorporated in Singapore should implement a group policy to ensure that all intragroup entities are complying with the notice requirements. However, a branch located overseas can decide not to comply with the outsourcing agreement terms of the notice provided that the bank proves that the risks are still covered.



II - Material ongoing outsourced relevant services (MOORS)

a. Policies and procedures

MAS requires banks to produce policies and procedures to identify material ongoing outsourced relevant services, assess related risks and monitor them. In case of any disruption, the policies and procedures should document business continuity measures and procedures to follow in case of any disruption.

b. Evaluation framework and due diligence

The notice mainly focuses on the bank's ability to manage outsourcing risk. Thus, it requires banks to develop a framework evaluating the outsourcing service provider's ability to perform its duties and to run a complementary due diligence to enhance scrutiny. The due diligence can be carried out by a third party under specific conditions detailed in the notice.

c. Use of sub-contractor

To protect customers' data and privacy, banks should, prior to calling on a sub-contractor, request the consent of the customer.

In case the material ongoing outsourced relevant services is sub-contracted, the bank must ensure that involving a sub-contractor will neither trigger significant risks for the banks (legal, reputational, technological, operational) nor for the confidentiality and integrity of information disclosed. This assessment should be documented and periodically reviewed.

d. Outsourcing agreement

MAS requires specific terms to be included by banks in the outsourcing agreement. The terms cover (i) confidentiality and integrity, (ii) information disclosure, (iii) Audit, (iv) termination of outsourcing agreement modalities.

Every intragroup entity acting on behalf of the bank must comply and include the terms stated in the notice in their outsourcing agreement.

e. Audit

Banks based in Singapore should conduct independent audit at least one every three years on material ongoing outsourced relevant services. Banks should also ensure that independent audits are also conducted in intragroup entities

f. Termination of services

When the service provider has failed to safeguard the confidentiality of information or if its ability to safeguard the confidentiality has deteriorated, a bank is required to consider the termination of the contract and document its considerations.

Once the agreement is terminated, all customers' information should be removed from the possession of the service provider and either deleted or destroyed.

g. Overseas regulated financial institution

When dealing with a service provider or sub-contractor overseas, the bank should notify the MAS within 14 days after disclosure of customers information and ensure the protection and accessibility of the information. Specific procedures and policies on customer information management are set out in the Notice.

III - Outsourced relevant services that involve the disclosure of customer information.

This category involves all outsourced relevant services beside material ongoing outsourced relevant services.

It is subject to general requirements with respect to:

- ❖ evaluation of service providers,
- ❖ outsourcing agreement,
- ❖ protection of the customer information, and
- ❖ termination of the services.

Conclusion and recommended next steps

The notice and the outsourcing guideline for banks introduce significant changes, particularly in the distinction between different outsourcing categories and the application of varying requirements based on the category. This includes an increased focus on "material ongoing outsourcing related services" (MOORS).

The following steps are recommended for banks to start their journey toward outsourcing compliance by:

- ❖ Assess and scope their third-party service providers to identify outsourcing categories applicable to outsourced services.
- ❖ Identify the gaps between their current operating model and the requirements.
  This includes:
  - ○ Revisit the internal outsourcing register to meet the expanded documentation and reporting requirements of the Notice.
  - ○ Review group policies to incorporate MAS amendments for outsourcing processes and third-party risk management.
  - ○ For banks headquartered outside Singapore, a gap analysis should also include a comparison with the home regulator's expectations to ensure compliance with both local and global requirements.
- ❖ Review the overall governance with definition of the board and senior management roles and responsibilities.

To meet the stricter requirements for MOORS, banks should consider additional steps, such as:

- ❖ Design an evaluation framework including recurring due diligence processes that are applied to each outsourcing arrangement and service provider.
- ❖ Update outsourcing agreements according to the notice requirements (confidentiality, contract termination, etc.)
- ❖ Engage with customers for seeking approvals for the disclosure of customer data to a service provider where required.
- ❖ Implement associated processes and policies for group and intragroup entities.
- ❖ If not yet implemented: define frequency and scope for independent audit.

The following table contains an overview of the detailed expectations and recommended actions.

Considering the Notice's and Guidelines' effective date in December 2024, banks should be completing their gap and impact analysis right now and move towards implementing the changes in the second and third quarter.

Understanding the impact of the new MAS outsourcing Notice for banks			
Notice section	**Description**	**Deliverable**	**Recommended implementation actions**
Monitoring and control of outsourced relevant services	Internal registry of outsourced relevant services obtained from a service provider	Register	- Periodical update of the register. - Semi-annual submission to the authority.
Group policy covering outsourced relevant services	Group policy implementation	Group policy	- Ensure each intragroup entity complies with the requirements.
Material ongoing outsourced relevant services (MOORS)	Manage material ongoing outsourced relevant services	Policies and procedure	- Identify the relevant services. - Implement adequate monitoring. - Establish measures to minimise potential disruption.
	Evaluation of service providers	Framework	- Evaluate the outsourcing service provider's ability to perform its duties. - Perform due diligence checks (if not performed by a third party).
	Requirements regarding the use of sub-contractor	Documented assessment	- Risk assessment of sub-contracting arrangement (legal, technological, reputational, operational, business, confidentiality). - Periodical review of the assessment.
	Access to information	Outsourcing agreement	- Include specific terms mentioned in the Notice
	Customer protection	*Not specified*	- Implement adequate measures to protect customer information
	Audit of material ongoing outsourced relevant services	Audits report	- Conduct independent audits on each of the services and document it. - Ensure independent audits are conducted in intragroup entities.
	Material ongoing outsourced relevant services obtained from an Overseas regulated financial institution	Procedure and policies	- Document policies on disclosure management of customers information. - Inform authority of customer information disclosure within 14 working days.
Outsourced relevant services that involve the disclosure of customer information	Evaluation of service provider relating to outsources relevant services	Due diligence check	- Ensure the confidentiality and secure disclosure of customers information (if not performed by third party).
	Access to information	Outsourcing agreement	- Include specific terms mentioned in the Notice
	Customer protection	*Not specified*	- Implement adequate measure to protect customer information

Implementation of Operational Resilience Standards in Hong Kong – learnings from BCBS' adoption assessment

In early 2021, the Basel Committee on Banking Supervision (BCBS) published the Principles for Operational Resilience (POR) and the revised Principles for the Sound Management of Operational Risk (PSMOR) in order to promote banks' ability to deliver critical operations through disruptions or operational risk-related events and improve banks' effectiveness in operational risk management.

In late 2023, the Committee assessed the adoption of these principles, with results showing disparity in terms of effectiveness and maturity between banks and across jurisdictions.

Overview of the BCBS principles

The PSMOR establish principles for operational risk management. The POR sets out a principles-based approach to improving operational resilience which is an outcome of good operational risk management and the ability to response to and recover from material incidents and disruptions.

The POR are composed of 7 principles: POR 1 on Governance, POR 2 on Operational risk management, POR 3 on Business continuity planning and testing, POR 4 on Mapping interconnections and inter-dependencies, POR 5 on Third party dependency management, POR 6 on Incident management and POR 7 on Information and communication technology (ICT).

The PSMOR are composed of 12 principles: PSMOR 1 on Risk management culture, PSMOR 2 on Operational risk management framework, PSMOR 3, 4, 5 on Governance, PSMOR 6 on Identification and assessment, PSMOR 7 on Change management, PSMOR 8 on Monitoring and reporting, PSMOR 9 on Control and mitigation, PSMOR 10 on ICT, PSMOR 11 on Business continuity planning relationship and PSMOR 12 on Disclosure.
These BCBS principles serve as guidelines for many regulators around the world, including the HKMA (Hong Kong Monetary Authority).

BCBS observations from November 2023 and their learnings for banks in Hong Kong

Banks in Hong Kong need to achieve operational resilience by 2026, following HKMA's Supervisory Policy Manual OR-2 on Operational Resilience. BCBS' assessment of worldwide implementation aspects and observed shortcomings provides important lessons learned and good practices that banks should incorporate in the course of their implementation:

Dedicated governance

Most banks have established proper operational risk management governance (PSMOR 3, 4, 5), as opposed to operational resilience governance (POR 1), which is not always defined and implemented.

In Hong Kong, for instance, the HKMA expects involvement from the banks' Board and senior management who are expected to actively participate in defining, implementing and supervising the operational resilience framework.

Consideration of business continuity and ICT within the operational resilience framework

Business continuity practices and ICT management have been well adopted by most banks following the principles for operational risk (PSMOR 11 and PSMOR 10). However, the adoption of the corresponding POR on business continuity and testing (POR 3) and ICT (POR 7) is still presenting challenges for banks.

Mapping of interconnections and interdependencies with the right granularity and relevant scenario

According to BCBS' assessment, most banks have failed to deliver a mapping that is granular enough to cover the end-to-end view of critical operations, their complexity and the scope of people, processes and systems involved (POR 4). They also faced difficulties in defining scenarios that meet the plausibility and severity expectations.
Under HKMA's requirements, such mapping should also identify risks and events that may impact the deli-

-very of critical operations. They also expect banks to conduct periodic scenario testing to assess their ability to stay operationally resilient over the long term.

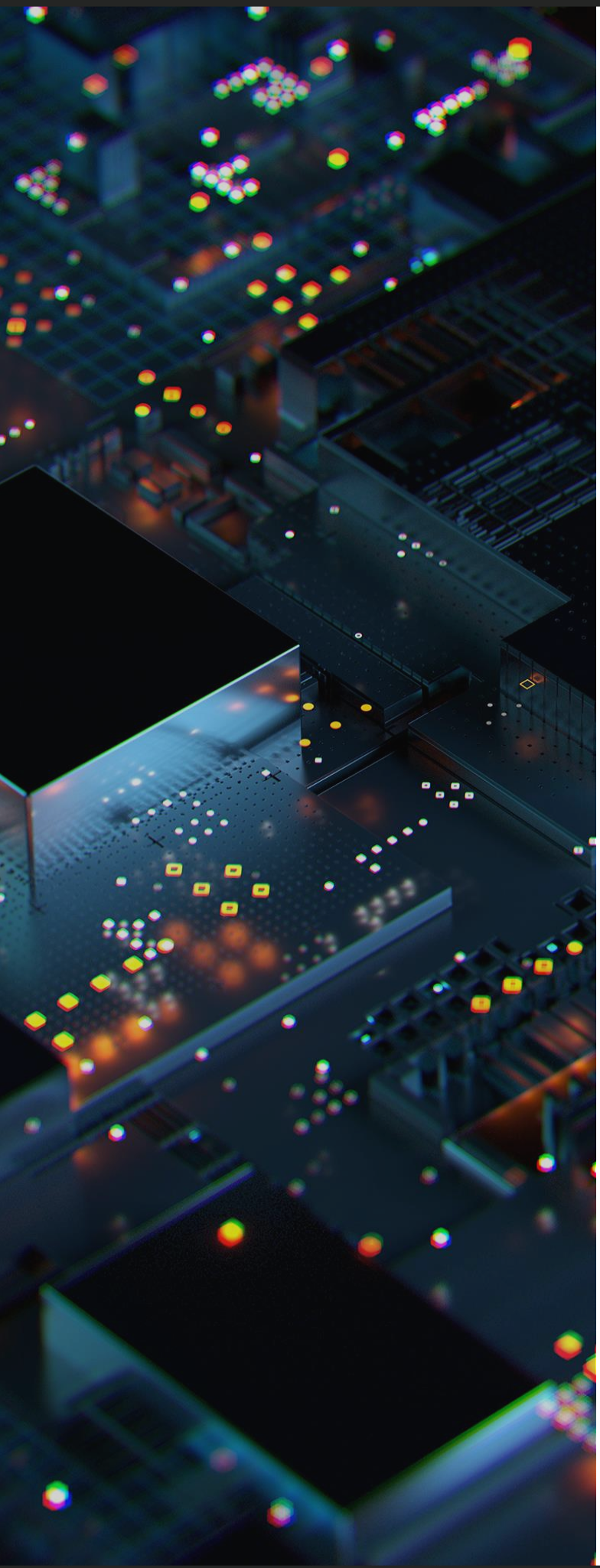
Third parties' integration into the operational resilience framework

Another major challenge lies in the management of third parties and their alignment with resilience expectations (POR 5 and PSMOR 9), especially when third parties are responsible for delivering or contributing to the delivery of critical operations.

The HKMA has warned against conducting business with a third party that may weaken the operational resilience of the banks' critical operations and affect its viability or role in the local financial system.

Key learnings for achieving Operational Resilience in Hong Kong

OR framework component	HKMA requirement	BCBS observations	Implications for banks
End-to-end view of critical operations and risk management	1. Identify and mitigate risks that may threaten the delivery of critical operations	Most banks failed to deliver a granular end-to-end view of critical operations, their complexity, and the scope of people, processes and systems involved in their mapping of interconnections and interdependencies.	The HKMA requires a mapping at a level of granularity which allows the bank to assess impact of risks, identify weaknesses, facilitate scenarios testing and be able to execute the recovery. Banks should review their current mapping against these requirements and avoid the shortcomings BCBS observed in the market.
Tolerance for disruption and definition of severe and plausible scenarios	2. Reinstate delivery of critical operations when disruptions occur, including under severe but plausible scenarios	Setting and testing the Tolerance for disruption are key prerequisites for operational resilience and should drive decisions about measures and investments for improved resilience. A poor definition or implementation could threaten the effectiveness of banks' risk management. In this context, BCBS noted that banks are struggling with the plausibility and severity of their scenarios.	When setting tolerance for disruption, the HKMA requires at least a time-based metric and suggests using other quantitative and qualitative indicators. In conjunction with insights from scenario testing, these metrics should drive and facilitate (management) decisions in the context of operational resilience.
Incident management	3. Resume normal operations in a timely manner after disruptions occur	An incident's severity must be classified according to predefined criteria such as the expected time to return to BAU (POR 6).	Banks should review their existing incident management processes, with a focus on the full life cycle of incidents, their prioritization and the ability to respond and recover in line with their tolerance and other metrics. Both HKMA and BCBS emphasize that current practices do not always prioritize and allocate resources properly.
Lessons learned	4. Absorb learnings from disruptions or near misses to continually improve its ability to prevent, adapt to and recover from risks and disruptions to critical operations delivery	The importance of learning and adjusting the operational resilience framework is at the core of the BCBS principles, reported in several principles, notably in the Incident management principle (POR 6).	Both HKMA and BCBS highlight that proactive learning from both scenario testing and actual incidents should be implemented to improve the operational resilience framework, the ability to prevent, adapt to and recover from future disruptions. Achieving operational resilience is a continuous, iterative process rather than a linear one.



Review of incident management practices

BCBS highlights the necessity for banks to adopt better incident management practices (POR 6), citing the proliferation of large-impact operational risk events in recent years.

Review of banks' risk and control self-assessments for critical operations

Banks have been leveraging their Risk and Control Self-Assessment (RCSA) processes to evaluate their risk exposure in the context of critical operations (POR 2). However, the BCBS identified areas for improvement in terms of capabilities and effectiveness.

Key considerations for a successful implementation of the operational resilience requirements

Step 1 – Choosing the right parameters

Banks aiming to be operationally resilient need to choose their operational resilience parameters wisely. As foundation of the operational resilience framework, banks need to identify their critical operations, tolerances for disruption and define severe but plausible scenarios.

Defining the most relevant parameters requires clear communication and alignment with stakeholders, consideration of the organization's unique business model as well as anticipation and flexibility that allows reprioritization in case of macro-economic change.

SPM OR-2 required the definition of these parameters by May 2023 while operational resilience should be achieved by 2026.

Based on the BCBS assessment, banks are encouraged to reassess their operational resilience parameters as a core component of their framework and improve their implementation accordingly.

Critical operations

The HKMA expects banks to identify critical operations whose disruption could threaten a bank's viability or the wider financial system.

This should reflect the organization's business model and function within the financial system and consider its activities under the critical functions identified in their recovery plan.

In recovery and resolution planning, critical functions may include, for instance:

- deposit business,
- lending business,
- transaction services (inc. e.g. payment and clearing), and
- money market and capital market activities.

Tolerances for disruption

Tolerances for disruption should be set strategically and serve as drivers for resilience-related decisions. The BCBS re-emphasized their role in the decision-making process, while acknowledging that their definition can be challenging.

In addition to time-based metrics, tolerance for disruption can also relate to the maximum tolerable number of customers affected by a disruption, the maximum number of transactions affected by a disruption, and the maximum value of transactions impacted, for instance.

Severe but plausible scenarios

Scenario testing is an established practice in business continuity planning and management. However, recent events have highlighted shortcomings in covering risks with high impact and low probability (black swan), such as the pandemic or the Ukraine war. It is no coincidence that regulators and standard-setters, starting with the BCBS and the Bank of England issued their operational resilience principles in 2021, reflecting experiences from the COVID-19 pandemic.

The following list illustrates examples of triggers for severe but plausible scenarios :

- multi-point impact from materializing risks,
- critical third-party failures or material incidents,
- disruption or failure in internal or external physical or technical infrastructure,
- workforce unavailability issues,
- cyber incidents, and
- internal or external fraud cases.

Scenarios design should include the type, speed, severity and time horizon, the logical sequence and timeline of stress events, with detailed description and quantitative parameters at each time period.

Banks need to document the considerations, processes and assumptions underpinning the selection and design of the scenarios.

When defining and testing the scenarios, banks should consider the financial and operational impact, assess the adequacy of the recovery indicator and governance frameworks and the recovery strategy and capacity.

Step 2 – Mapping of interconnections and interdependencies in the delivery of critical operations

Nearly three years after the BCBS issued its principles on operational resilience, it found that some banks still fail at delivering a granular end-to-end mapping of interconnections and interdependencies underlying their critical operations delivery. The BCBS observes that this mapping and the definition of tolerances for disruption represent the most common challenges for banks aiming to adopt the principles.

Banks need to identify people, processes and systems underlying the previously defined critical operations. The complexity is increased when the bank outsources to third parties with multiple layers involved. Interdependencies exist with their outsourcing guidelines and third-party risk management.

Step 3 – Leveraging on the existing risk management

Operational risk management

An advanced and consistent framework for managing non-financial risks (such as operational risk, third-party risk, ICT risk, and BCM) will help banks achieve operational resilience by providing relevant inputs for scenario testing, risk responses, potential mitigants and recovery options.

Vice versa, implementing the operational resilience framework will also inform and enhance regular non-financial risk management, reducing potential impacts from materializing risks in the future.

Business continuity management

Business continuity planning focuses on the planning and operationalization of crisis responses and resumption of operations.

Operational resilience, on the other hand, focuses on the viability of the bank and its impact on the financial system in case of disruption. It references to and integrates elements from risk management and bank's recovery and resolution plans.
In the context of operational resilience, BCM is a tool intertwined with the operational resilience framework, helping to become operationally resilient. While BCP is, to some extent, a reactive approach, operational resilience is proactive.

Third-party dependency management

Where the delivery of critical operations depends on services provided by third parties, banks should review SLAs, contracts and assess the resilience of the third parties, e.g. via their BCPs.

As part of the third-party risk management and in the course of the scenario testing, banks will have to engage critical vendors and/or assess how operations could be transferred seamlessly in cases of disruption.
This is even more accentuated in the case of multi layered third-party involvement.

Information and Communication Technology

A bank should ensure that its information and communication technology and data management are robust, resilient and subject to protection, detection, response and recovery plans.

As part of the mapping process, a bank should identify where technology is part of the delivery of critical operations. The identified applications and infrastructure should be tested as part of the execution of severe but plausible scenarios. On-going threat intelligence and situational awareness plans should be part of ICT risk management and the operational resilience framework.
Metrics such as Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) need to be reassessed against the tolerance parameters to ensure adequate allocation of staff and technical resources.

Step 4 – Testing the ability to deliver critical operations during disruption

The testing phase refers to the simulation of severe but plausible scenarios, the assessment of the outcomes and the processing of learnings. It is crucial as it allows organizations to assess their readiness and

ability to deliver critical operations in an adverse environment.
The BCBS highlighted challenges that banks face in defining scenarios. However, it is crucial for banks to rigorously define adequate scenarios due to the strategic importance of operational resilience. This ensures that scenarios remain relevant and applicable when risks materialize.
For simulating scenarios, banks need to decide between desktop testing and real simulation testing.
The former option is less costly and less resource-intensive but may overlook important aspects of real-life situations. In contrast, the latter option is more realistic and engaging but requires significant resources and time.

Step 5 – Incident detection, response and recovery

A review should be performed on the existing incident detection and reporting including real- or near-time monitoring of incidents and operational risks. Response procedures should also be reviewed to reassess the governance, processes, and information flows required to respond to disruption.

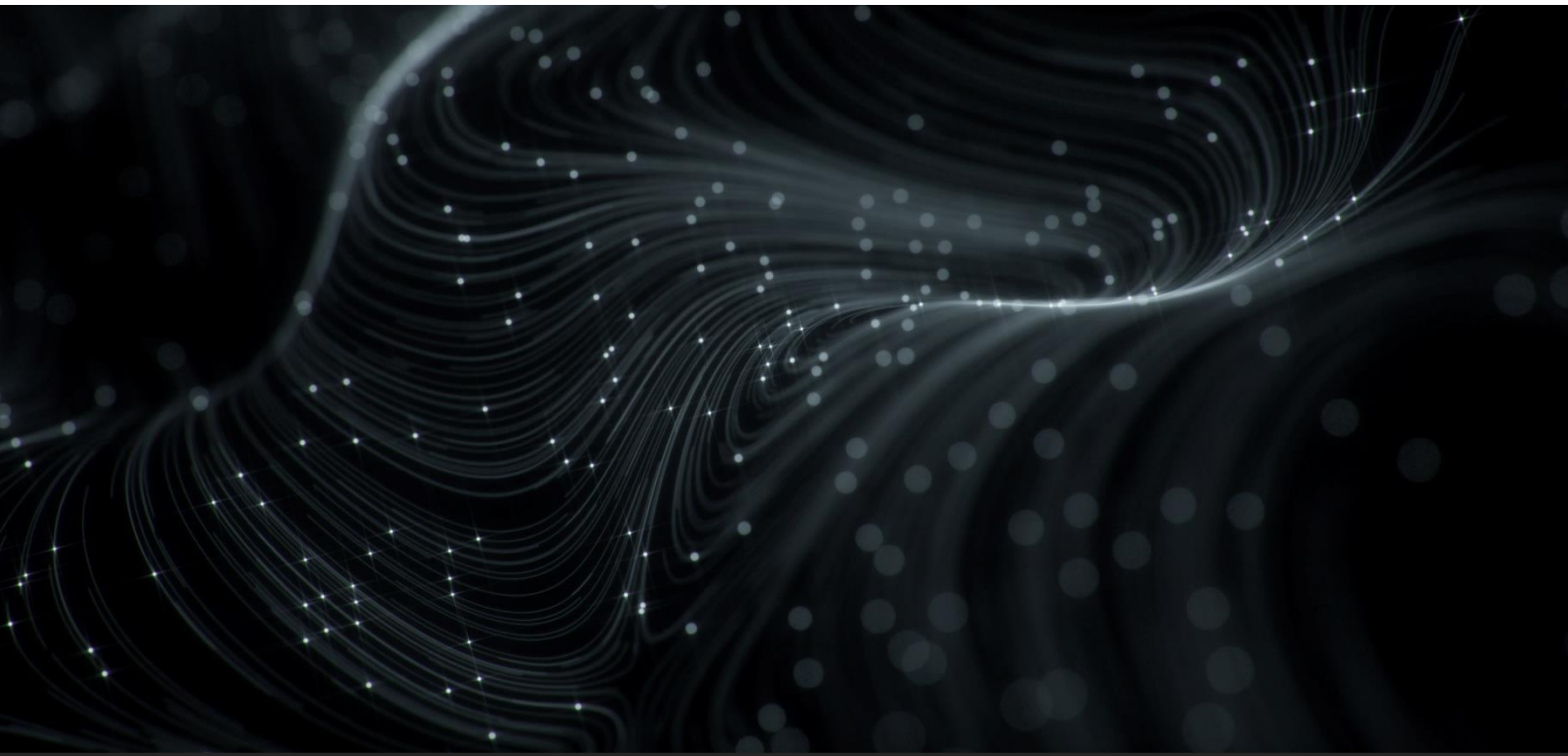
Communication is a key aspect during any crisis. The communication plan needs to be reviewed to ensure aspect such as customer support prioritization, remote capabilities and control room are integrated.
Following the resolution of incidents, it is essential to investigate and document the root causes and identify learnings for future incident prevention. Banks can also consider using tools and techniques such as RPA or process mining to analyse historic and prevent future incidents.

Conclusion

The operational resilience framework is a proactive approach to achieving operational resilience by anticipating, preparing, responding to and recovering from an incident.
In addition to meeting compliance requirements, operational resilience is crucial for ensuring a bank's viability. It should be an integral part of its culture, mission, strategy, and day-to-day management.

To achieve operational resilience and comply with HKMA's expectations, banks should process BCBS' latest insights, review and continue implementing the key aspects of their operational resilience framework. This includes, but is not limited to defining critical operations, tolerances for disruptions and severe but plausible scenarios as well as integrating the framework with existing risk management and incident response practices.

Lastly, organizations should avoid viewing operational resilience as a one-time exercise. While achieving operational resilience by or before 2026 is an important milestone, it should be seen as an ongoing, iterative process. This process should include regular reviews of the framework and the incorporation of insights and lessons learned from risks and incidents.



REGTECH CORNER

Kaiko

For this issue's Regtech corner, we interviewed Sean Lawrence, Kaiko's Head of APAC, a digital assets market data provider, offering enterprise-grade data infrastructure to institutional clients. Kaiko is located in Paris, London, New York and Singapore.

About Sean Lawrence,
Kaiko, Head of APAC

Sean is a 30-years veteran of financial markets, including positions as CEO of ABN AMRO Clearing Tokyo and APAC Regional Head of ETD Operations at UBS.

Aurexia: Can you provide a brief overview of Kaiko and its value proposition for clients?

Kaiko: Kaiko bridges traditional and blockchain ecosystems by providing reliable and actionable financial data and services. Founded in 2014, Kaiko is the leading source of cryptocurrency market data, analytics, indices, and research, providing businesses with industrial-grade and regulatory-compliant data. Kaiko empowers market participants with global connectivity to real-time and historical data feeds for use cases across the investment lifecycle. We have physical offices in France (covering Europe), UK, US, Singapore and Hong Kong.

Kaiko also provides trusted information, from all markets, on all networks.

- *We are integrated everywhere:* Our goal is to enable every business to access market data from all centralized and decentralized platforms.
- *We are a leader in financial innovation*: This is made possible by our team of financial experts who work diligently to design products tailored to crypto assets.
- *We are bridging the gap between traditional and digital finance*: We lead projects to build the digital finance of tomorrow and create durable industry standards.
- *We are listening to the market*: All of our data products are built with our clients in mind for real use cases.

What specific challenges and opportunities do regulatory developments in the APAC region present for Kaiko?

Hong Kong is largely prescriptive, and adopting a "same activity, same risk, same regulation" approach to regulating the onshore virtual asset market. This creates a high barrier of entry for web3.0-native companies who are not set up to be as functionally operational as their traditional finance counterparts.

For example, web3.0-native exchanges are held to similar standards as the likes of Hong Kong Exchange with regards to strict financial and operational controls, along with independent checks and audits. This presents a strong business opportunity for Kaiko's audit-compliant pricing services to help companies comply with the licensing requirements. At the same time, the challenge is that we perceive that only a handful of applicants will eventually obtain the necessary licenses to operate.

Korea has been largely retail-speculative, although there is a tough stance on the asset class in the wake of the LUNA crash in 2022. We are observing the institutional market picking up, amidst possible regulatory tailwinds expected in the second half of this year.

Similarly, Thailand is retail-speculative and largely spot market-driven; there have been few broker licenses issued especially in the aftermath of the Celsius blowup which impacted local players like Zipmex. There has been quiet optimism since local players like Siam Commercial Bank have been building their commercial offerings.

Japan has a well-defined, policy driven approach to digital assets legislation/regulation. However, practical articulations of these make it difficult to see a sustainable business case for firms operating in Japan. For example, the requirement to back stablecoins with at least 100% fiat currency, makes the economics of a stablecoin to be questionable. Similarly, requiring all crypto assets to be held formally 'in trust' negates much of the benefits of blockchain to companies and investors.

REGTECH CORNER

Kaiko

Singapore's regulatory environment is largely very pro-blockchain but less so towards digital payment tokens such as cryptocurrency; MAS has expressly banned solicitation of retail business by digital payment token companies.

There is a separate digital payments token act that sets the rules of engagement for digital payment companies in Singapore. Meanwhile, MAS have been very proactive in encouraging the exploration of blockchain/DLT in capital markets and retail use cases via a sandbox/POC environment, which aligns with Kaiko's strategic business within the pricing oracle space.

Australia's regulatory landscape is largely politically-influenced. ASIC has taken a strong stance against regulating the scene; ACT and RBA are stepping up in various capacities. Trading volumes are low; institutions are dominated by local players with participation from few foreign companies. One clear challenge is the lack of clear rules of engagement for market participants.

How does Kaiko help its clients navigate and ensure compliance with the regulatory landscape in the APAC region?

Kaiko's SOC 2 Type 2 certification and audit-compliant Pricing Services help clients meet independent financial control as well as accounting requirements such as the impending FASB updates.
Also, our indices is AMF-licensed and supervised under EU BMR framework, to provide independent and manipulation-resistant benchmarks for structured products/ETP issuances.

What are Kaiko's future plans and strategies in response to anticipated regulatory changes or advancements in APAC?

Kaiko's current business model allows us to serve clients in both the traditional web2.0 and web3.0 world. For example, our data distribution channels include APIs (web2.0) and cloud (web2.0) as well as blockchain oracles (web3.0).

As we observe more regulatory clarity in various jurisdictions around digital assets, more licensed traditional finance players are entering the space; eventually most parts of the ecosystem will be dominated by licensed players.

Kaiko has been involved in the wider ecosystem. Could you elaborate on key strategic partnerships and collaborations that have contributed to the company's growth and success?

Kaiko's growth and success is in part attributed to various strategic/commercial partnerships, examples including but not limited to:

- Benchmark services and provision for structured products and derivatives: CBOE, Gemini, D2X, Bullish, Bitstamp.
- Data distribution partners: Bloomberg, IRESS, Deutsche Boerse, ICE Global Network, BT Radianz, IPC, Chainlink etc.
- Cross-selling of complementary products: OANDA for FX rates, TPICAP, etc.
- Price Display: Bloomberg, Messari etc.
- Other Strategic Partnerships: Nansen, Google etc.

Kaiko's offering for pricing & valuation of digital assets

Source: Kaiko

Sithi SIRIMANOTHAM
Partner & Group COO
sithi.sirimanotham@aurexia.com

Sebastian L SOHN
Director (Singapore)
sebastian.sohn@aurexia.com

Bringing value, Together

© 2024 Aurexia Pte Ltd. Material in this publication may not be copied, reproduced or republished in any way except for your own personal, non-commercial use. Prior written consent of Aurexia Pte Ltd must be obtained if you intend to reuse. The contents of this publication represent the views of Aurexia and should not be taken as advice or the provision of professional services in any way.

Aurexia Pte Ltd is a Private Limited company registered in Singapore. Aurexia Pte Ltd is part of the global Aurexia group, which also has offices in France, Luxembourg, United Kingdom, Canada, and Hong Kong.

Aurexia

Bringing value, together