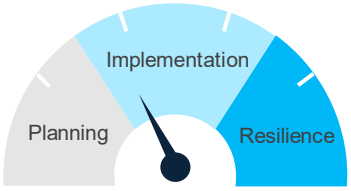
KPMG

Operational Resilience for Banks

Ensuring the delivery of critical operations throughout any potential disruption to services

November 2023

Operational Resilience (OR) has moved to the top of the agenda for banks since the HKMA issued the Supervisory Policy Manual (SPM) module *OR-2 Operational Resilience* on 31 May 2022. The city's banks have successfully met a key deadline in May this year to have their OR-2 frameworks and timelines in place, and are now ultimately working towards being operationally resilient by 31 May 2026.



Currently, we expect that the regulators will review and feed back the results from their August survey of banks' selections of critical operations, severe but plausible scenarios and tolerance for disruption. The OR-2 processes have demonstrated that operational resilience is not a one-off compliance exercise. Rather, it is an ongoing expectation that banks will be able to provide services to their customers throughout any severe disruptions. Learning from recent events, including the Covid-19 pandemic and the extreme weather in Hong Kong, banks must be prepared to manage all risks that have the potential to affect their delivery of critical operations.

The ongoing management and testing of OR frameworks is resource-intensive and will involve more efforts to align enterprise-wide roles and responsibilities. Forward-thinking banks should make use of technology to continuously embed resilience and other risk management capabilities. Banks should also allocate the right level of investment to be prepared to manage all incidents, especially those that may impact critical operations and cause intolerable harm to customers and risk to market integrity.

Ultimately, operational resilience not only benefits banks and protects their customers, but also plays a crucial role in strengthening the foundations of Hong Kong as a stable and secure global finance hub.

KPMG has been supporting clients to design and implement OR frameworks in Hong Kong and other jurisdictions with our Powered Resilience Solution. This solution is based on the successful delivery of OR frameworks to clients in the banking sector, regulatory insights and market leading practices..

Operational Risk Management (ORM)

As operational risk management and operational resilience are closely interconnected, the HKMA issued the revised Supervisory Policy Manual module OR-1 Operational Risk Management in July 2022 to provide banks with further guidelines on operational risk framework and to align with operational resilience.

Operational risk has become an increasingly important issue for banks as they are providing more services and products to their customers while relying on complex and automated technology as well as outsourcing some of their functions. Failure to implement proper processes and procedures to control operational risks can result in significant operational losses to banks, and impact their customers.

An effective operational risk management system and a robust level of operational resilience work together to reduce the frequency and the impact of operational risk events. Examples of such a system include:

Vulnerability assessment

Identify, assess, monitor and control the operational risk inherent in critical operations

Scenario analysis

Identify, analyse and measure a range of scenarios, including low probability but high severity events, which could result in severe operational risk losses

Review processes in change initiatives

Ensure procedures to identify and assess vulnerabilities would remain effective after a change to any underlying components (people, process, technology, information or facilities) of critical operations

The revised OR-1 clarifies existing principles, introduces advancements in change management and information and communication technology management, and provides specific guidance related to Operational Resilience. Banks are required to implement these changes by 25 January 2024 to ensure a seamless transition towards operational resiliency.

Business Continuity Planning and Testing

The HKMA issued the revised Supervisory Policy Manual module TM-G-2 Business Continuity Planning on 31 May 2022 to align with OR-2 for the purpose of ensuring critical operations delivery during disruptions. Business continuity planning (BCP) and testing supports the bank's ability to prepare for and recover from emergencies or disasters. It acts as the backbone for incident management and contributes to the bank's ability to continue delivering its critical operations through disruptions.

An effective BCP is forward-looking and should be validated for a range of severe but plausible scenarios which contain disruptive events and incidents. Examples of an effective BCP include:

1. Identifying critical operations as well as the key internal and external dependencies (people, technologies, information and facilities) supporting the critical operations delivery
2. Incorporating business impact analysis, recovery strategies, testing programmes, training and awareness programmes, communication strategies and crisis management processes
3. Ensuring that operations that are reliant on critical third-party services for delivery of critical operations are part of the BCP process

The revised TM-G-2 serves as the foundation for OR-2, introducing business continuity planning as a vital element of the operational resilience framework. TM-G-2 provides additional requirements and testing provisions, standardising the terminology used for business continuity planning and operational resilience. Banks are required to implement the module by 31 May 2026.

Third-Party Dependency Management

Banks are increasingly engaging third parties and often also rely on intragroup entities for the provision of services or delivery of functions. Banks should not enter into, or continue, any third party or intragroup arrangements that may weaken the operational resilience of the bank's critical operations.

Banks should endeavour to prevent disruptions at third parties or intragroup entities from affecting critical operations delivery. To minimise potential risks to critical operations, banks should manage their dependencies on third parties and intragroup entities with outsourcing arrangements. For example:

Prior to entering into third party arrangements

Verify whether the third parties or intragroup entities has at least an equivalent level of operational resilience to that of the bank in Hong Kong. Where such verification is not feasible, the bank should take alternative steps to satisfy itself that the engagement would not weaken its ability to deliver critical operations in the event of a disruption

During the course of engaging a third party or intragroup

Banks should have adequate arrangements in place to continually satisfy itself that the third party or intragroup entity has maintained an acceptable level of operational resilience - including when conducting scenario testing and enhancing workaround plans, or when a disruption occurs to the third party

Ongoing monitoring

Develop appropriate business continuity and contingency planning procedures and exit strategies to maintain operational resilience in the event of a failure or disruption at a third party or intragroup entity which may impact its delivery of critical operations

A growing reliance on third parties and intragroup entities means that banks' senior management must prioritise in areas to ensure continued service to customers, especially during disruptive external events. Ongoing monitoring is imperative to preserve the operational resilience of their banks' delivery of critical operations and to prevent any disruptions at group entities from affecting their own critical operations in Hong Kong.

Information and Communication Technology (ICT) including Cybersecurity

Growing technology adoption also raises the likelihood that a bank's critical operations may depend on, or be affected by lapses in, ICT risk management. While relying on technology support, banks should ensure the confidentiality, integrity and availability of clients' critical information assets.

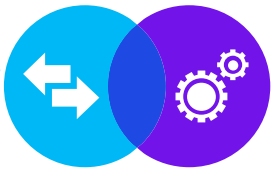
While automated processes are less prone to error than manual processes, they have the potential to introduce risks that must be addressed through sound ICT and cybersecurity management.

Information and Communication Technology (ICT) including Cybersecurity (continued)

Given the interconnections and interdependencies across technology and cloud in most, if not all, of banks' operations and resources (e.g. processes, people, information, facilities, third parties or intragroup entities), it is imperative for banks to use technology, data or tooling to manage resiliency and mitigate risks. Ensuring resiliency across complex and interrelated silos should be an ongoing consideration for banks and not viewed only as a compliance exercise.

To ensure the confidentiality, integrity and availability of data and systems, banks should also regularly review the effectiveness of their ICT risk management including the design and implementation. Examples of these include:

Regular alignment of the business, risk management and ICT strategies to ensure consistency with the bank's risk appetite and tolerance statement as well as with privacy and other applicable laws



Develop approaches to ICT readiness for stressed scenarios during disruptive external events, and severe but plausible scenarios. This could include implementing wide-scale remote access, rapid deployment of physical assets, and/or significant expansion of bandwidth to support remote user connections and customer data protection

How will technology address operational resilience challenges, especially after May 2026?

Banks will need to consider how they manage resiliency and incident management reporting and remediation going forward, to ensure controls and measures are in place, and actions are followed up by all reporting lines and for senior management– ensuring the priority of remedial actions by the board or board committee oversight.

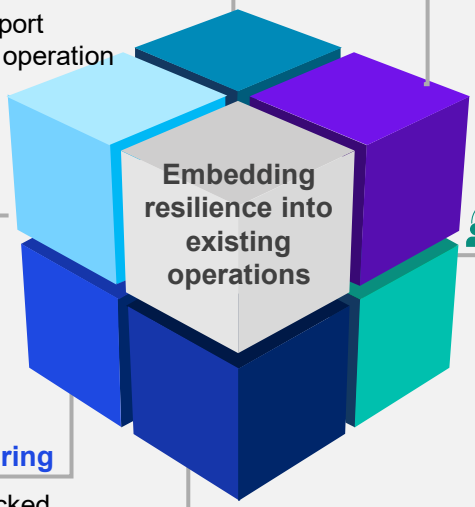
We recommend banks to use technology, data or tooling to continuously embed resilience and other related capabilities to integrate their operational resilience framework and ongoing management of vulnerabilities assessment into their existing incident management programme. There are six areas for consideration.

Clear Roles and Responsibilities

- **Clear segregation of roles and responsibilities** among management level, business units and supporting teams for transparency and oversight
- All relevant business and support functions supporting a critical operation are **assigned to individual responsibilities and tasks**

Change Management

- Establish workflows and tracked approvals for **audit trail**, updates or changes to Operational Resilience information (e.g. policy and procedures)



Review and Escalation

- **Access** the latest list of OR parameters, incident logs and formal reports of scenario testing results, where required.

Optimal Resources Allocation

- The data and tooling platform can act as **a repository of the Operational Resilience data** and information, such as the list of OR parameters, mapping documentation and audit trail

Tracking and Risk Monitoring

- **Risk indicators** can be tracked automatically in the data and tooling platform for respective stakeholders to identify potential vulnerabilities and follow-up on the remedial actions

Comprehensive Mapping Documentation

- The system allows a clear visualisation of display between relationships of the **mapping of interconnections and interdependencies** among the operational processes and its supporting assets underlying critical operations delivery

KPMG has a global, multi-disciplinary team with subject matter advisors who have significant depth and capability across the resilience, operational risk, business continuity plan and management, recovery and resolution planning, cyber and technology domains. We draw on this depth 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 banking sector, please contact us:

Tom Jenkins
Partner, Head of Banking and Asset Management Risk Advisory, Hong Kong
KPMG China
E. tom.jenkins@kpmg.com

Cara Moey
Director, Operational Resilience Solution Lead, Hong Kong
KPMG China
E. cara.moey@kpmg.com

Lanis Lam
Partner, Technology & Cyber Resilience Lead
Hong Kong
KPMG China
E. lanis.lam@kpmg.com

Gemini Yang
Partner, Risk Consulting, Hong Kong
KPMG China
E. gemini.yang@kpmg.com

Hubert Hui
Associate Director, Operational Resilience SME, Hong Kong
KPMG China
E. hubert.hui@kpmg.com

Dunkan Hu
Associate Director Management Consulting, Hong Kong
KPMG China
E. dunkan.hu@kpmg.com

kpmg.com/cn/socialmedia

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