KPMG

Operational Resilience

A principles-based approach to strengthening operational resilience in the global banking system

August 2020

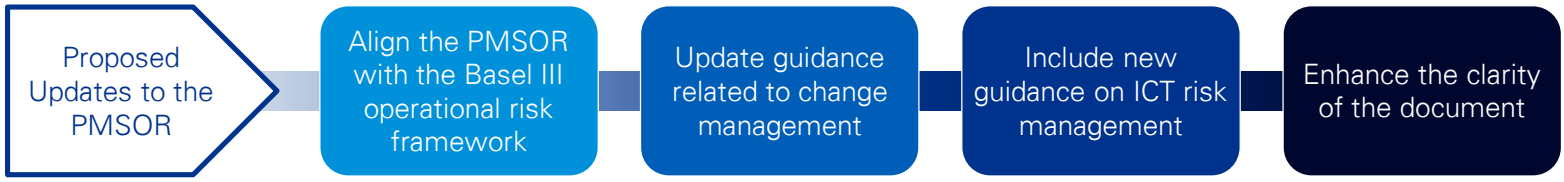
The Basel Committee for Banking Supervision (BCBS) released a consultative document outlining their principles for operational resilience[1] on 6 August 2020. Banking regulators in key jurisdictions (including Hong Kong) are expected to implement operational resiliency requirements in due course once the Basel Committee has finalized the consultative process.

The BCBS has noted that higher levels of capital and liquidity have improved banks' ability to absorb financial shocks, but they believe that further work is necessary to strengthen banks' ability to absorb operational risk-related events, such as pandemics, cyber incidents, technology failures or natural disasters. These severe events could trigger significant operational failures or wide-scale disruptions in financial markets. The COVID-19 pandemic provides a clear example of how operations can be impacted by severe operational risk-related events and the need for banks to rapidly adapt their operational posture. Recognising that a range of potential hazards cannot be prevented, the Committee believes that a pragmatic, flexible approach to operational resilience can enhance the ability of banks to withstand, adapt to and recover from potential hazards and thereby, mitigate potentially severe adverse impacts.

Operational Resilience and the Evolution of Operational Risk Management

The Committee defines operational resilience as the ability of a bank to deliver critical operations through disruption. 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 to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should take into account its overall risk appetite, risk capacity and risk profile.

In addition to the operational resilience principles, the BCBS has proposed updates to the *Principles for the Sound Management of Operational Risk* (PMSOR)[2]. The proposed updates to the PMSOR are intended to address areas where, based on a 2014 BCBS review of 60 institutions, banks were found to need additional guidance to facilitate implementation of the principles.



Principles for Operational Resilience

Operational Resilience Principles	Considerations for Designing the Operational Resilience Framework
Principle 1: Governance Banks should utilise their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on delivering critical operations through disruption.	• The Board of directors is responsible for reviewing and approving the bank's operational risk expectations considering the bank's risk appetite, risk capacity, and risk profile. • A broad range of "severe but plausible" scenarios should be considered when formulating the bank's risk tolerance for disruption to its critical operations.
Principle 2: Operational Risk Management Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience expectations	• The operational risk management function should work with the respective functions (defined to include functions within the three lines of defense, consisting of business unit management, an independent operational risk management function, and independent assurance) to coordinate business continuity planning, third-party dependency management, recovery and resolution management, and other relevant risk management frameworks, as appropriate. • Controls and procedures should be sufficient to identify external and internal threats and vulnerabilities in people, processes, and systems in a timely manner.
Principle 3: Business Continuity Planning and Testing Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.	Business continuity plans should: • Be in place and exercises should be regularly conducted under a range of "severe but plausible scenarios" of potential disruption to critical operations • Include impact analyses, recovery strategies, testing programs, training and awareness programs, and communication programs • Provide implementation guidance for the disaster recovery framework, establish roles and responsibilities for managing the disruption and succession of authority. • Set out decision-making processes and define triggers for invoking the plan.
Principle 4: Mapping interconnections and interdependencies Once a bank has identified its critical operations, it should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations.	• The respective functions should document internal and external interconnections and interdependencies, including people, technology, processes, information, and facilities involved in delivering critical operations. • The approach and granularity should be sufficient to identify vulnerabilities and support testing to stay within the risk tolerance levels.
Principle 5: Third-party dependency management Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intra-group entities, for the delivery of critical operations.	• Prior to entering into a third-party arrangement, the bank should verify whether the third party has operational resilience conditions to safeguard the bank's critical operations that are equivalent to those of the bank. • Arrangements should be formalized through written agreements that cover how to maintain operational resilience in both normal circumstances and in the event of a disruption. • Business continuity plans should consider exit strategies for third parties, as well as assess the substitutability of a third party in the event of a failure or outage at that third party, as well as other viable alternatives.
Principle 6: Incident Management Banks should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the bank's risk tolerance for disruption considering the bank's risk appetite, risk capacity and risk profile. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.	• An incident response and recovery plan should be developed to manage incidents; it should be periodically reviewed, tested, and updated, including updates based on lessons learned directly and indirectly. • The scope of the incident management plan should cover the life cycle of an incident, including classification of the severity based on pre-defined criteria; thresholds for triggering business continuity, disaster recovery, and crisis management procedures; and implementation of communication plans to report incidents internally and externally, and determine lessons learned.
Principle 7: ICT including cyber security Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant information to users on a timely basis in order to fully support and facilitate the delivery of the bank's critical operations.	• Banks should have a documented ICT policy, including cyber security, stipulating governance and oversight, risk ownership and accountability, information security, periodic testing and monitoring, and plans for incident response, business continuity, and disaster recovery. • Dependencies on critical information assets and infrastructure should be identified and cyber security efforts should be prioritized based on the significance of critical information assets to critical operations, including protection of data integrity and confidentiality. • Plans to facilitate wide-scale remote access, rapid deployment of physical assets, or significant expansion of bandwidth to support remote user connections and customer data protection should address: Risk mitigation strategies, defined processes for management of remote assets, users, and application development and regular updates to maintain security posture.

Adopting these principles also brings business benefits

We can see that a broader approach to operational resilience is paying off. A more coordinated approach coupled with business or service simplification can result in efficiency and cost savings. A strategic and analytics-driven process can allow for better customer and supplier experience and more dynamic risk management. In addition, a strong and coordinated framework helps with regulatory compliance. With an increased regulatory focus on resilience as well as likely ongoing disruption, it makes sense to tackle this topic today.

- Allow better work in a dynamic ecosystem e.g. use of Fintech and start-ups
- Generate synergies across strategic, financial and operational resilience
- Reduce operational risks and the costs of disruption
- Enhance Governance and inter-regional/ global collaboration
- Allocate resources more effectively and efficiently
- Improve supplier and third party relationships
- Enhance customer (buy-side and sell-side) trust and loyalty

How KPMG can help

Third party risk management

- Supply Chain Management
- Third party risk strategy, operating model and tooling

Effective Governance

- Resilience strategy
- Governance
- Policies and procedures
- Resilience culture and awareness
- Regulatory requirements

Recovery and response

- Crisis management
- Incident response
- BCP and Disaster Recovery
- Communication management
- Talent management

Target Operating Model

- Governance
- Organisational accountability, roles and responsibilities
- Legal entity and booking strategy
- Location strategy
- Customer Experience
- Critical service definition
- Process and systems alignment
- Business case definition

Analytics

- Data requirements assessment
- Data Management
- Management reporting and KPIs

End-to-end testing

- Tolerance setting
- Scenario analysis
- Risk based test plan
- Testing execution

Contacts

Isabel Zisselsberger
Partner,
Head of Management Consulting
KPMG China
T: +852 2826 8033
E: isabel.zisselsberger@kpmg.com

Tom Jenkins
Partner,
Head of Financial Risk Management
KPMG China
T: +852 2143 8570
E: tom.jenkins@kpmg.com

Sean Ren
Associate Director,
Management Consulting
KPMG China
T: +852 3927 5818
E: sean.ren@kpmg.com

James Philpott
Manager,
Financial Risk Management
KPMG China
T: +852 3927 5828
E: james.philpott@kpmg.com