KPMG

Regulatory Alert

Regulatory Insights

August 2020

Proposed Principles of Operational Resilience and Operational Risk

Basel Committee proposals seek to strengthen banks' ability to withstand significant operational failures or wide-scale disruptions.

Key points

- COVID-19 has exacerbated operational risks, especially dependencies on technology and third-party service providers, and increased economic and business uncertainty.
- The Basel Committee has proposed seven principles for operational resilience intended to help banks strengthen their ability to withstand, adapt to, and recover from operational risk-related events, such as pandemics, cyber incidents, technology failures, or natural disasters.
- Proposed updates to the principles for operational risk, or PMSOR, have been issued concurrently and include updates on change management and a new principle on information and communication technologies.

The Basel Committee on Banking Supervision (Basel Committee or BCBS) has issued two consultative documents seeking comment on proposed *Principles for Operational Resilience* and updates to its *Principles for the Sound Management of Operational Risk* (PMSOR). The Basel Committee views operational resilience to be an outcome of effective operational risk management and, as such, has drafted the two documents to work together. In addition, each draws upon existing guidance and current practices (including principles-based guidance on corporate governance, business continuity, and outsourcing) in an effort to develop a "coherent framework." Comments are requested by November 6, 2020.

Principles for operational resilience

The Basel Committee defines operational resilience as "the ability to deliver critical operations through disruption." Impact from COVID-19 has shown that while capital and liquidity requirements have improved banks' ability to absorb financial shocks, more work is needed to strengthen their ability to absorb—that is, respond and adapt to, and recover and learn from—operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets. These events would include pandemics, cyber incidents, technology failures, or natural disasters. BCBS has proposed a principles-based approach to operational resilience covering the following seven categories. Key features of each principle are also highlighted.

1. *Governance*
   - 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.

2. *Operational risk management*
   - 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.

3. *Business continuity planning and testing*
   - 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.

4. *Mapping interconnections and interdependencies*
   - 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.

5. *Third-party dependency management*
   - 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.

6. *Incident management*
   - 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.

7. *Resilient information and communication technology (ICT), including cyber security*
   - 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

– Regular updates to maintain security posture.

Principles for the sound management of operational risk

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. These areas included: 1) operational risk identification and assessment; 2) change management; 3) operational risk appetite and tolerance; and 4) disclosure. At that time, the Basel Committee also found that a specific principle on ICT risk management was warranted.

The currently proposed updates would:

— Align the PMSOR with the Basel III operational risk framework
— Update guidance related to change management
— Include new guidance on ICT risk management
— Enhance the clarity of the document.

As drafted, the new ICT principle 10, Information and communication technology, would read:

> *Banks should implement robust ICT governance that is consistent with their risk appetite and tolerance statement for operational risk and ensures that their ICT fully supports and facilitates their operations ICT should be subject to appropriate risk identification protection detection, response and recovery programs that are regularly tested, incorporate appropriate situational awareness, and convey relevant information to users on a timely basis.*

Basel Committee on Banking Supervision

The Basel Committee is a global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen regulation, supervision, and practices of banks worldwide with the purpose of enhancing financial stability.

The BCBS has 45 members comprised of central banks and bank supervisors from 28 jurisdictions. It does not have any formal supranational authority and its decisions do not have legal force. Rather, the BCBS relies on its members' commitment to work together to contribute to the developments of BCBS standards and sound practices as well as implement and apply these standards and practices in their domestic jurisdictions.

For additional information please contact Brian Hart or Greg Matthews.

Amy Matsuo
Principal and National Lead
Regulatory Insights
T: 919-664-7302
E: amatsuo@kpmg.com

Contributing authors:
Amy Matsuo, Principal and National Lead, Regulatory Insights

Karen Staines, Director, Regulatory Insights

kpmg.com/socialmedia