BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

Principles for operational resilience – Executive Summary

The *Principles for operational resilience* (the POR) were published in 2021 and build on the Basel Committee on Banking Supervision's *Principles for the sound management of operational risk* (the PSMOR), originally issued in 2011, revised in 2014 and revised a second time simultaneously with the issuance of the POR.

While the PSMOR establish principles for operational risk management, the POR seek to promote a principles-based approach to improving operational resilience as an outcome of effectively managing operational risks that may arise from disruptions, such as pandemics, natural disasters, cyber attacks or technology failures.[1] The approach adopted by the POR reflects banks' experiences during the Covid-19 pandemic and their increased dependence on third parties for the provision of financial services.

The POR define operational resilience as a bank's ability to deliver critical operations in the face of disruption. This ability should enable a bank to identify and protect itself from threats and potential failures. Moreover, it should allow the bank to respond, adapt to, recover and learn from, disruptive events to reduce their impact on the delivery of critical operations in the face of disruption.[2] Banks should assume that disruptions will occur and define their overall risk appetite and "tolerance for disruption" accordingly. The POR define tolerance for disruption as the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios.

The POR should be applied consistently across the organisation on a consolidated basis consistent with the scope of the Basel Framework, and with due consideration of the bank's recovery and resolution plans.

The seven principles of the POR

The POR's seven principles are as follows:

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 role of a bank's board includes approving the bank's operational resilience approach, which should consider the bank's risk appetite and tolerance for disruption to its critical operations. In formulating the bank's tolerance for disruption, the board of directors should consider the bank's operational capabilities given a broad range of severe but plausible scenarios that would affect its critical operations.
- Senior management is responsible for the implementation of the bank's operational resilience approach, clear communication and appropriate allocation of resources.

[1] The 12 principles established in the PSMOR cover governance, risk management environment, information and communication technology (ICT), business continuity and the role of disclosure.

[2] The term critical operations is based on the 2006 high-level principles for business continuity of the Joint Forum, which includes the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS). The term encompasses critical functions as defined by the Financial Stability Board and is expanded to include activities, processes, services and their relevant supporting assets, the disruption of which would be material to the continued operation of the bank or its role in the financial system.

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 approach.*

- Banks' operational risk management functions are to be coordinated with other relevant functions, such as third-party dependency management and recovery and resolution planning.
- Banks should have controls and procedures to identify and assess threats, and to the extent possible, prevent them from affecting critical operations. These controls and procedures should be assessed regularly and, in particular, in response to changes to any underlying components of their critical operations and after incidents to take account of lessons learned.

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 identify critical operations and key dependencies, and internal decision-making processes should be based on forward-looking triggers and disruption assessments.
- Business continuity plans should establish the roles and responsibilities for managing operational disruptions and provide clear guidance regarding the succession of authority in the event of a disruption that impacts key personnel.
- Roles and responsibilities, including succession planning for key personnel, should be defined.

Mapping interconnections and interdependencies: *Once a bank has identified its critical operations, the bank should map the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.*

- Mapping implies identifying and documenting people, technology, processes, information and facilities relevant for critical operations, including those operations that depend on third parties.
- Recovery and resolution plans should be leveraged for definitions of critical operations.
- The approach and level of granularity of mapping should be sufficient for banks to identify vulnerabilities and to support testing of their ability to deliver critical operations in the face of disruption.

Third-party dependency management: *Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intragroup entities, for the delivery of critical operations.*

- Before entering third-party arrangements, banks should perform risk assessment and due diligence and verify whether the third party has at least an equivalent level of operational resilience.
- Business continuity and contingency planning procedures and exit strategies should be developed so that banks can maintain their operational resilience if disruptions at a third party impact critical operations.
- Banks should assess the substitutability of critical third parties, including reverting to in-house options.

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 appetite and tolerance for disruption. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.*

- Banks should maintain inventories of incident response and recovery resources.
- Incident reports should capture the life cycle of an incident and assess severity and incident reporting.
- Incident response procedures should be reviewed periodically to prevent serial recurrence.
- Incident management should reflect lessons learned from past incidents and those learned by others.

Information and communication technology (ICT) including cyber security: *Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that (i) are regularly tested, (ii) incorporate appropriate situational awareness and (iii) convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the bank's critical operations.*

- A documented ICT policy should cover all relevant aspects, including governance and risk ownership.
- Banks should identify critical information assets and the infrastructure upon which they depend.
- Banks should develop plans and implement controls to maintain the integrity of critical information.
- Banks should evaluate the threat profile of their critical information assets and test for vulnerabilities.

This Executive Summary and related tutorials are also available in FSI Connect, the online learning tool of the Bank for International Settlements.