April 2024

Workshop 3
Operational resilience

Chair: Ben Gully, Deputy Superintendent – Supervision Sector, Office of the Superintendent of Financial Institutions (OSFI)

The *Core Principles for effective banking supervision* (BCP) have been revised to reflect developments in operational resilience, including through the introduction of a new CP25 Operational risk and operational resilience. Significant efforts have been directed at strengthening operational resilience, to ensure that banks are better able to withstand, adapt to and recover from severe operational risk-related events, such as those arising from pandemics, cyber incidents, technology failures or natural disasters. The new CP25 retains the key requirements relating to operational risk, while also enhancing the focus on governance, operational risk management, business continuity planning and testing, mapping interconnections and interdependencies, third-party dependency management, incident management and resilient cyber security and information and communication technology (ICT).

Following the Global Financial Crisis, and exacerbated by the growth of technology-related threats, the Covid-19 pandemic and rising geopolitical risk, the operational resilience of banks has become a key supervisory priority. More and more banks are facing the risks of large-scale business disruption due to systems failure, increasingly diverse cyberattack incidents, terrorism, regional conflicts, and natural disasters. All of which have tested their operational resilience and demonstrated how crucial resilience is in the current environment. At the same time, banks are relying increasingly on third or fourth parties in their business operations, which increases the complexity of operations and makes it difficult to analyse the root cause and impact of incidents that arise.

Cases in which customers are adversely affected by lengthy recovery times following system failures or temporary service outages are increasingly observed in the banking sector.[1] At the same time, the ability of supervisors to prepare for and respond to these instances is impaired by:

- the wide range of scenarios faced by banks, which can vary by nature, severity, and speed;
- systemic impacts (eg incidents involving a critical third party or subcontractor);
- lags in incident reporting to supervisors;
- the potential need to share information and coordinate responses across multiple regulators and jurisdictions; and
- supervisory resource and expertise constraints.

[1] Recent examples include:

- Technology outages affecting banks' retail banking operations, such as online banking services.
- Outages affecting third-party data centres, resulting in an inability to access payment services at multiple banks.
- Outages affecting telecommunications companies, resulting in widespread service disruptions to banks' call centres, telephone and SMS services, and payments services.
- Ransomware attacks disrupting clearing and settlement activities, resulting in the use of untested manual workarounds.

Committee work on operational resilience

The new CP25 is closely aligned with the Committee's *Principles for Operational Resilience* (POR).[2] Through the publication of the POR, the Committee sought to promote a principles-based approach to improving banks' operational resilience. The POR should be applied consistently across the banking group on a consolidated basis consistent with the scope of the Basel Framework, and with due consideration given to the bank's recovery and resolution plans.

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. 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 build upon the Committee's revised *Principles for the Sound Management of Operational Risk* (PSMOR)[3] and are largely derived and adapted from existing guidance on outsourcing, business continuity, and risk management-related guidance issued by the Committee and national supervisors. 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, or technology failures. 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 focus on governance; operational risk management; business continuity planning and testing; mapping interconnections and interdependencies; third-party dependency management; incident management; and resilient cyber security and ICT.

Progress made by banks to adopt the POR

The POR are not a complete reinvention of banks' management of operational resilience. Many elements were already in place when the Principles came into force. The challenge is to integrate and coordinate the various operations (eg ICT, business continuity). To evaluate the adoption of the POR, the Committee carried out an assessment among its members in early 2023.[4] The results of this assessment indicate that:

- Board members' roles and responsibilities and capabilities for operational resilience are still under development (POR 1).
- Banks have leveraged Risk and Control Self-Assessments (RCSAs) to identify threats and vulnerabilities to the delivery of critical operations (POR 2), but there are gaps in capabilities and effectiveness.
- In most jurisdictions, banks' mapping of interconnections and interdependencies (POR 4) does not provide a sufficiently granular end-to-end view of critical operations, their complexity, and supporting people, processes and systems.

[2] BCBS (2021a).

[3] BCBS(2022b).

[4] See BCBS (2023).

- For the principles on business continuity and testing (POR 3) and ICT (POR 7), banks are still facing challenges (eg consideration of end-to-end delivery of critical operations, and the plausibility and severity of scenarios). Some banks have started to incorporate operational resilience into existing ICT risk management frameworks.
- The management of third parties and dependencies (POR 5) is considered to be among the most significant challenges for banks. For some banks, there is still work to do on developing appropriate business continuity and contingency plans and exit procedures where third parties provide critical operations.
- The continuous growth of operational risk-related events has heightened the necessity for banks to identify and respond to these incidents and crises, resulting in generally well-established incident management practices (POR 6) in nearly all jurisdictions.

The assessment also revealed several themes that have proved to be particularly relevant for the adoption of the Principles:

- First, it is crucial for banks to leverage all aspects of operational risk management to achieve operational resilience and to recognise its importance alongside financial resilience.
- Second, banks should acknowledge that operational resilience is more than just business continuity. A key differentiator is the critical operations lens (in conjunction with the end-to-end view), the focus on impact, the use of the tolerance for disruption to drive decisions about resilience investment, and the consideration of third parties' resilience.
- Finally, banks should establish and maintain accurate data at an appropriate level of granularity on critical operations and recognise the foundational role of mapping interconnections and interdependencies for successfully adopting the Principles.

Operational resilience environment

Q1. What are the top current and emerging threats to banks’ operational resilience in your jurisdiction?

Q2. What kinds of disruptions to banking services have you experienced in your jurisdiction in the past year? How did banks respond to these disruptions?

Implementation challenges

Q3. Can you share examples of successful initiatives implemented by banks to enhance their operational resilience?

Role of supervisors

Q4. How is operational resilience embedded in your jurisdiction’s supervisory approach?

Q5. How does your jurisdiction ensure that supervisors have the right capabilities in operational resilience (eg training, recruitment, talent management)?

References

Basel Committee on Banking Supervision (2021a): “Principles for operational resilience”, March.

——— (2021b): “Revisions to the principles for the sound management of operational risk”, March.

——— (2023): “Supervisory newsletter on the adoption of POR and PSMOR”, November.