Principles for the Sound Management of Operational Risk (PSMOR) – Executive Summary

In March 2021, the Basel Committee on Banking Supervision (BCBS) published its *Revisions to the Principles for the Sound Management of Operational Risk* (PSMOR). The principles were introduced in 2003 and subsequently revised in 2011 to incorporate the lessons from the Great Financial Crisis. The 2021 revisions resulted from a 2014 review that indicated that several principles had not been adequately implemented and did not sufficiently capture certain important sources of operational risk.

Operational risk is inherent in all banking products, activities, processes and systems. Sound operational risk management reflects the effectiveness of the board of directors and senior management in administering their portfolio of products, activities, processes and systems.

The PSMOR and its regular updates aim to promote the effectiveness of operational risk management throughout the banking system. They reflect sound practices relevant to all banks. However, the BCBS recommends that banks should take account of the nature, size, complexity and risk profile of their activities when implementing the principles.

The 12 principles

The 12 principles of the 2021 PSMOR cover governance, the risk management environment, information and communication technology (ICT), business continuity planning and the role of disclosure. These elements should not be viewed in isolation; rather, they are integrated components of the bank's operational risk management framework (ORMF) and its overall risk management framework (including operational resilience).

Principle 1 emphasises the role of the board in promoting a strong risk management culture in the bank

The board of directors should take the leading role in establishing a strong risk management culture, implemented by senior management. The board should establish and regularly review and approve core policies (including risk management, compensation, code of conduct or ethics policies). Through these policies, the board and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behaviour, and ensure that staff receives appropriate risk management and ethics training.

Principle 2 provides general requirements for the ORMF

Banks should develop, implement and maintain an ORMF that is fully integrated into the bank's overall risk management processes by the first line of defence, adequately reviewed and challenged by the second line of defence and independently reviewed by the third line of defence. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile.

Principle 3 describes the board's main duties with respect to the ORMF

The board of directors should approve and periodically review the ORMF. The board should also ensure that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.

Principle 4 sets guidance regarding the bank's risk appetite and tolerance statement

The board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume. The risk appetite and tolerance statement for operational risk should be easy to communicate and understand. Moreover, it should include key background information and assumptions, be forward-looking and clearly articulate the motivations for taking on or avoiding certain risks. It should also establish boundaries or indicators to enable monitoring of these risks.

Principle 5 describes senior management's duties relating to the effective implementation of the ORMF

Senior management should develop for approval by the board a clear, effective and robust governance structure, commensurate with the nature, size, complexity and risk profile of the bank's activities. Its role is also to translate the ORMF (approved by the board of directors) into specific policies, procedures and processes and ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and resources.

Principle 6 sets guidance for the identification and assessment of operational risk

Senior management should ensure the comprehensive identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. Examples of tools used for identifying and assessing operational risk include event management, operational risk event data, self-assessments of both operational risks and controls, control monitoring and assurance frameworks, operational risk metrics, scenario analysis, benchmarking and comparative analysis.

Principle 7 deals with change management

Senior management should ensure that the bank has policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change on the basis of agreed objective criteria. Change implementation should be monitored by specific oversight controls. Change management policies and procedures should be subject to independent and regular review and update and should clearly allocate roles and responsibilities in accordance with the three-lines-of-defence model.

Principle 8 sets guidance for operational risk monitoring and reporting

Senior management should implement a process to regularly monitor operational risk profiles and material operational exposures. Appropriate reporting mechanisms should be in place at the board of directors, senior management and business unit levels to support proactive management of operational risk. Operational risk reports should include:

- breaches of the bank's risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements
- a discussion and assessment of key and emerging risks
- details of recent significant internal operational risk events and losses (including root cause analysis)
- relevant external events or regulatory changes and any potential impact on the bank

Principle 9 describes the control environment and risk mitigation

Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies. A sound internal control programme requires appropriate segregation of duties and consists of four components that are integral to the risk management process: risk assessment, control activities, information and communication, and monitoring activities. In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party, such as through insurance.

Principle 10 highlights the importance of ICT risk management for the operational risk profile of the bank

Effective ICT performance and security are paramount for a bank to conduct its business properly. Therefore, banks should implement a robust ICT risk management programme in alignment with their operational risk management frameworks. The board of directors should regularly oversee the effectiveness of the bank's ICT risk management. Senior management should routinely evaluate the design, implementation and effectiveness of the bank's ICT risk management to ensure data and systems' confidentiality, integrity and availability.

Principle 11 establishes the relationship between ORMF and business continuity planning

Banks should prepare forward-looking business continuity plans (BCPs) with scenario analyses associated with relevant impact assessments and recovery procedures. Banks should periodically review their BCPs and policies to ensure that contingency strategies remain consistent with current operations, risks and threats. BCPs should be linked to bank ORMFs.

Principle 12 describes the role of disclosure

Banks should disclose their ORMFs in a manner that allows stakeholders to determine whether the banks identify, assess, monitor and control/mitigate operational risk effectively. Banks should disclose relevant operational risk exposure information to their stakeholders (including significant operational loss events), while not creating operational risk through this disclosure (eg description of unaddressed control vulnerabilities). A bank should have a formal disclosure policy that is subject to regular and independent review and approval by senior management and the board of directors.

Role of supervisors

The PSMOR require supervisors to regularly assess banks' ORMFs by evaluating their policies, processes and systems related to operational risk. Supervisory evaluations of operational risk should include all areas described in the PSMOR. In certain circumstances, supervisors may choose to use external auditors in these assessment processes. Supervisors should take steps to ensure that banks address deficiencies identified through the supervisory review of banks' ORMFs.

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