BCBS
Revisions to the Principles for the Sound Management of Operational Risk

August 2020

pwc

Executive Summary

As a key risk class, operational risk is notoriously 'light' on requirements, the Principles for the Sound Management of Operational Risk (PSMOR) provides the clearest official articulation of international good industry practice and regulatory expectations for banks, the broader financial services industry and regulators. Therefore, changes to it may have a material impact on operational risk practitioners (Line 1 & 2), senior managers and boards.

The Basel Committee on Banking Supervision (BCBS) published the PSMOR in 2003 to provide a framework of principles related to operational risk to guide industry practitioners and supervisors. The BCBS updated the principles in 2011 and conducted a review of the implementation in 2014. In August 2020 the BCBS published a further revision to the PSMOR for consultation, with comments to be provided by 6 November.

The proposed changes to the PSMOR include the following:

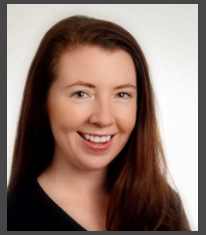
- **Incorporation of further guidance following the 2014 implementation review**
  Further guidance related to risk identification and assessment tools, the role of risk in change management, further detail on the articulation of risk appetite, the use of scenario analysis and the introduction of operational risk exposures into disclosure requirements.
- **Roles and Responsibilities**
  There is increased emphasis on the role of senior management in the execution of operational risk management activities and greater specificity on the role of the board of directors. There is also a clearer articulation of the role of the three lines of defence in practice.
- **Sources of Risk**
  There is acknowledgement that the sources of operational risk have evolved. The introduction of information and communication Technology (ICT) risk provides for a greater articulation of principles specific to the management this risk type.
- **Operational Resilience**
  Given the increased recognition of the severity of operational disruptions, the BCBS has developed a separate document on operational resilience; consequently operational resilience is removed from the scope of this paper.

An analysis of changes to each principle can be found on the following slide.

Principle	What has changed
Principle 1 Risk Culture	• New wording places the emphasis on senior management's responsibility to implement a strong risk culture and the steps the board of directors must take to facilitate this. • Clarity that poor risk culture includes inappropriate provision of financial services (whether wilful or negligent). • Added recommendation that the Code of Conduct should be reviewed and approved by the board, attested to by employees, its implementation overseen by a senior ethics committee, and be publicly available. • Management should now set clear accountabilities so bank staff understand their roles and responsibilities for risk management. • Clarity that customised training programmes should be mandatory for specific roles (e.g. heads of business units).
Principle 2 Operational risk management framework (ORMF)	• Addition of a recommendation for the board of directors and management to understand the nature and complexity of risks inherent in their systems. • Clarity that integration of ORMF into the bank's overall risk management processes is the first line's responsibility. • Added detail on inclusions to the ORMF, including: mandates and membership of operational risk governance committees; reference the relevant operational risk management policies and procedures; increased focus on control identification and assessment; and the approach to ensuring controls are designed, implemented and operating effectively. • Requires that policies be reviewed and revised, as appropriate, based on the continued assessment of the quality of the control environment, addressing internal and external changes.
Principle 3 The Board of Directors	• Change in emphasis on board responsibility and movement to greater ownership by senior management . For example, the board's role is now articulated as oversight of material operational risks and effectiveness of key controls, and ensuring senior management implement the ORMF. • Additional recommendation for the board to ensure controls 'be regularly reviewed, monitored and tested to ensure ongoing effectiveness'.
Principle 4 Risk Appetite	• There are new recommendations that the operational risk appetite should: be easy to communicate and understand; include key background information and assumptions; clearly articulate the motivations for assuming or avoiding certain types of risk, and the boundaries or indicators to monitor these risks; ensure the strategy and risk limits of each business unit and legal entity, as relevant, align with the bank-wide risk appetite statement; and be forward looking and, where applicable, subject to scenario and stress testing.
Principle 5 Senior Management	• The previous title was 'Three lines of defence and senior management', now this only references senior management. Wording related to the three lines of defence has been removed from the principle and detail has been added to the front of the document, where it is stressed that the three lines of defence model should be adequately and proportionally used by financial institutions to manage every kind of operational risk sub-category, including ICT risk.
Principle 6 Identification and Assessment in BAU	• Substantive changes to the list of tools used to identify and assess risk. Changes include: the removal of audit findings and capital as an example tool to identify and assess risk; further detail on the qualitative and quantitative analysis involved in the RCSA process and the documentation required; the addition of 'event management'; addition of control monitoring and assurance framework requiring a 'structured approach to the evaluation, review and ongoing monitoring and testing of key controls, sufficiency of control coverage' and that 'control monitoring should be appropriate for the different operational risks and key controls'; more detail has been provided on scenario analysis, specifically how to conduct scenarios and potential uses; and the addition of 'benchmarking' in the comparative analysis section. • Addition of the specification that data to be accurate and subject to the Corporate Operational Risk Function (CORF) monitored action plans and remediation plans where necessary.
Principle 7 Identification and Assessment in Change	• Greater clarity on the three lines of defence during change. Line 1 should perform the initial assessment; Line 2 conducts review and challenge of all stages of the process and ensures all control groups are involved as appropriate. • New recommendation to assess the evolution of associated risks from inception to termination (i e. throughout the full life-cycle of the product). • Addition of paragraph 40 'Banks should maintain a central record of their products and services to the extent possible (including the outsourced ones) to facilitate the monitoring of changes'. • Change management policies and procedures should be subject to independent and regular review and update.
Principle 8 Monitoring and Reporting	• The onus of the principle has been moved to senior management and removal of the word 'losses' from the principle, broadening it. • Detail makes it clear that Line 1 should be conducting 'reporting on any residual operational risks, including operational risk events, control deficiencies, process inadequacies and non-compliance with operational risk tolerances' • Addition of text on 'a discussion of key and emerging risks assessed and monitored by metrics' and the need to report on 'root cause analysis' for significant events and losses.
Principle 9 Control and Mitigation	• Removal of detail regarding technology risk (now it is clarified that they must follow the same process as operational risk) • New wording around concentration risk and the complexity of outsourcing. • The addition of paragraph 54 'banks should have unified classification, methodology, procedures of operational risk management established by the CORF'.
Principle 10 ICT	• New principle stating: '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 programmes that are regularly tested, incorporate appropriate situational awareness, and convey relevant information to users on a timely basis'
Principle 11 Business continuity planning	• The previous principle was titled 'business resiliency and continuity plans', the 'resiliency' wording has been dropped and separate principles are to be provided in the Principles for Operational Resilience paper.. • There is new text now on the need for board and senior management involvement in reviewing and implementing business continuity plans (BCP). • Clarity that BCP must be grounded in scenario analysis and the need to now set thresholds and limits for the activation of BCP.
Principle 12 Disclosure	• New wording around including operational risk exposures in disclosures. Historically banks have only disclosed their processes and capital holdings for operational risk. Now it is recommended that bank's include operational loss events, while not creating additional operational risk through this disclosure (e.g. description of unaddressed control vulnerabilities). This may be a material shift in reporting.

For more information and to discuss how this impacts you, please contact:

Paul Atkinson
Partner, Resilience & Risk Management
Mobile: +44 7764958656
Email: paul.j.atkinson@pwc.com



Jess Sparksman
Senior Manager, Non-Financial Risk Management
Mobile +44 7843332449
Email: jessica.sparksman@pwc.com

www.pwc.com