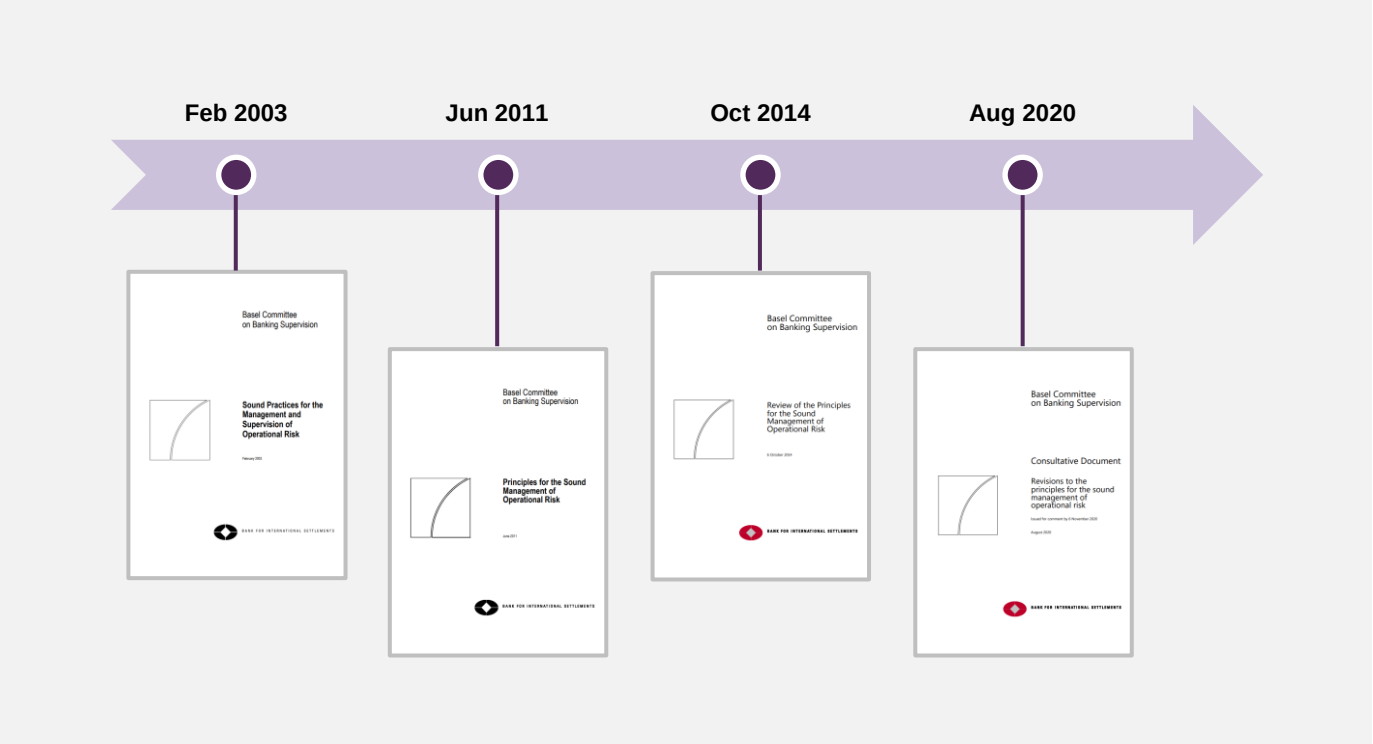
OPERATIONAL RISK – MITIGATING DISRUPTION

INTRODUCTION

In August 2020, the Basel Committee on Bank Supervision (BCBS) published a *Consultative Document*[1] on the Revisions to the Principles for the Sound Management of Operational Risk (PSMOR), with the purpose of providing guidance on the implementation of some of these principles as well as addressing some aspects of operational risk that were not sufficiently captured before. The guidance highlights the importance of developing and maintaining an efficient Operational Risk Management Framework (ORMF). In particular, it addresses five areas where the BCBS expects banks to follow better operational risk practices: Governance, Risk Management Environment, Information and Communication Technology (ICT), Business Continuity Planning and the Role of Disclosure.

[1] Consultative Document: Revisions to the principles for sound management of operational risk, 6 August 2020, https://www.bis.org/bcbs/publ/d508.pdf

Figure 1: *Timeline of Operation Risk Publications issued by the BCBS*



As this is an iterative approach to effectively managing operational risk, many of the principles in this document existed in previous publications – a timeline of publications is illustrated in Figure 1. The BCBS first published its PSMOR in 2003[2]. It subsequently updated the principles in 2011[3] and conducted a review of the implementation in 2014[4]. In this sense, the proposed revisions to the PSMOR published in August 2020 can be seen as evolution rather than revolution. The key proposed revisions to the PSMOR are presented in Table 1 and a thorough discussion about the changes in all principles follows.

Table 1: Key proposed revisions to the PSMOR (2020)

1. Increased emphasis is put on the role of senior management regarding the implementation of the ORMF
2. Change management is highlighted as an area of growing significance
3. The rising importance of ICT as a component of operational risk has led to the introduction of a new principle to cover this
4. Given the importance of operational disruptions, operational resilience is not included in the scope of this paper and separate principles are provided in the Principles for operational resilience paper (released together)
5. Improvements in transparency to stakeholders are encouraged through additional disclosure requirements

[2] Consultative Document: Sound Practices for the Management and Supervision of Operational Risk, 25 February 2003, https://www.bis.org/publ/bcbs96.pdf
[3] Consultative Document: Principles for Sound Management of Operational Risk, 30 June 2011, https://www.bis.org/publ/bcbs195.pdf
[4] Consultative Document: Review of the Principles for Sound Management of Operational Risk, 6 October 2014, https://www.bis.org/publ/bcbs292.pdf

GENERAL PRINCIPLES

PRINCIPLE 1 – OPERATIONAL RISK CULTURE: *The board of directors should take the lead in establishing a strong risk management culture, implemented by senior management. The board of directors 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.*

The proposed revisions:

- emphasise the actions the board and senior management should take to facilitate a sound risk management culture
- recommend that the Code of Conduct should be regularly reviewed and approved by the board and attested by employees; its implementation should be overseen by a senior ethics committee and should be publicly available
- mention that the Code of Conduct should prohibit conflicts of interest or the inappropriate provision of financial services (whether wilful or negligent)
- suggest that management should set clear expectations and accountabilities, so bank staff understand their roles and responsibilities for risk management
- explain that customised training programmes should be mandatory for specific roles (e.g. heads of business units, heads of internal controls and senior managers)

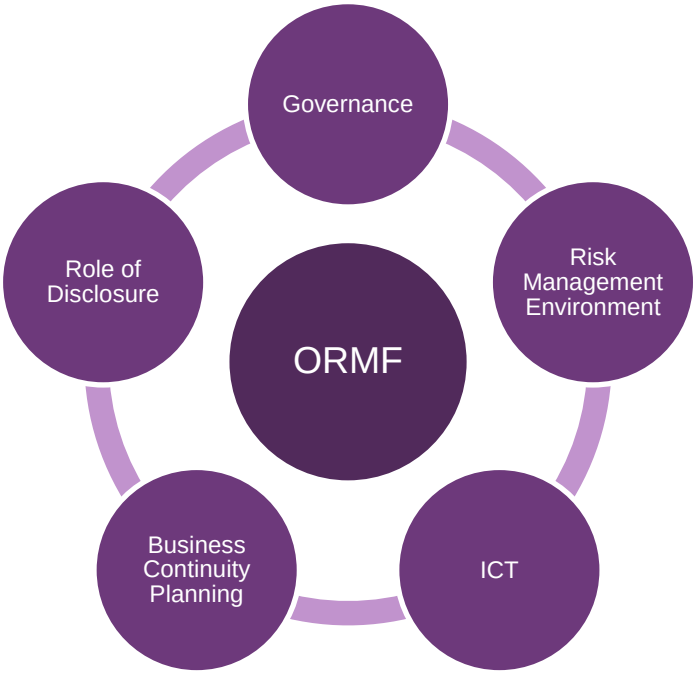
PRINCIPLE 2 – ORMF: *Banks should develop, implement and maintain an ORMF that is fully integrated into the bank's overall risk management processes. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile.*

The proposed changes:

- state that the board and management should understand the nature and complexity of the risks inherent in the portfolio of bank products, services, activities, and systems
- indicate that the components of the ORMF should be fully integrated into the overall risk management processes of the bank 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.
- recommend that the ORMF should be embedded across all levels of the organisation including group and business units as well as new business initiatives' products, activities, processes and systems
- suggest that the ORMF documentation should clearly identify the governance structures used to manage operational risk, reference the relevant operational risk management policies and procedures, describe the tools for risk and control identification and assessment, and report the bank's approach to ensure controls are designed, implemented and operating effectively
- require that policies be reviewed and revised, as appropriate, based on continued assessment of the quality of the control environment, addressing internal and external environmental changes

Figure 2 illustrates the five areas where the BCBS expects from banks to follow better operational risk practices. The paper continues by reviewing the proposed revisions to the specific principles related to each one of the ORMF elements.

Figure 2: *ORMF Elements*



GOVERNANCE

PRINCIPLE 3 – BOARD OF DIRECTORS: *The board of directors should oversee material operational risks and the effectiveness of key controls, and ensure that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.*

The board of directors should:

- ensure that the operational risk management processes are subject to comprehensive and dynamic oversight
- provide senior management with clear guidance regarding the principles underlying the ORMF, implying that senior management undertakes greater ownership
- regularly review, monitor and test controls to ensure ongoing effectiveness

PRINCIPLE 4 – OPERATIONAL RISK APPETITE AND TOLERANCE: *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.*

An effective risk appetite and tolerance statement should:

- be easy to communicate and understand
- include key background information and assumptions that informed the bank's business plans
- clearly articulate the motivations for taking on or avoiding certain types of risk and establish boundaries or indicators to enable monitoring of these risks

- ensure the strategy and risk limits of each business unit and legal entity align with the bank-wide risk appetite statement
- be forward-looking and, where applicable, subject to scenario and stress testing

PRINCIPLE 5 – SENIOR MANAGEMENT: *Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the bank's risk appetite and tolerance statement.*

Senior management should:

- develop and effectively implement the ORMF policies, processes and systems throughout all organisational levels and make sure that they are consistent with the bank's level of risk tolerance and risk appetite statement
- provide effective oversight for the risks inherent in a business unit's activity
- ensure the quality of the risk identification and assessment process, regular monitoring and comprehensive reporting of the operational risks and material exposures aiming to support proactive risk management, appropriateness of internal controls and mitigation strategies employed
- build a robust risk governance structure by considering the bank committee's structure, composition and operation

RISK MANAGEMENT ENVIRONMENT

PRINCIPLE 6 – RISK IDENTIFICATION AND ASSESSMENT: *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.*

The proposed revisions that reinforce the importance of risk identification and assessment tools include:

- further detail on the qualitative and quantitative analysis involved in the risk and control self-assessment process
- the introduction of 'event management'
- the addition of the control monitoring and assurance framework
- more detail on scenario analysis
- the incorporation of 'benchmarking' in comparative analysis

Banks should ensure that the operational risk assessment tools' outputs are based on accurate data, adequately taken into account in the internal pricing and performance measurement mechanisms and subject to the corporate operational risk management function's monitored action plans or remediation plans when necessary.

PRINCIPLE 7 – CHANGE MANAGEMENT: *Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and include continuous risk and control assessments, adequately articulated between the relevant lines of defence.*

The proposed changes:

- enhance the three lines of defence model during change. In particular, the first line should perform operational risk and control assessments of new products and initiatives, whereas the second line should challenge the operational risk and control assessments of the first line during all phases of the process and ensure that all control groups are involved as appropriate
- recommend that change management should assess the evolution of associated risks across time, from inception to termination
- state that banks should maintain a central record of their products and services to the extent possible to facilitate the monitoring of changes
- suggest that change management policies and procedures should be subject to independent and regular review and update

PRINCIPLE 8 – 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.*

The proposed revisions:

- provide senior management with greater responsibility
- explain that the first line of defence should ensure reporting on any residual operational risks, including operational risk events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances
- mention that reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions
- make clear that data capture and risk reporting processes should be analysed periodically with the goal of continuously enhancing risk management performance

PRINCIPLE 9 – CONTROL AND 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.*

The proposed changes:

- state that the board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities while taking into consideration the concentration of risk and the complexity of outsourcing
- suggest that banks should have unified classification, methodology, procedures of operational risk management established by the corporate operational risk management function

ICT

PRINCIPLE 10 – ICT: *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.*

This is a new principle that was added to the principles included in the Review of the Principles for Sound Management of Operational Risk (2014). The ICT framework set by the banks should:

- be reviewed on a regular basis for completeness against relevant industry standards and best practices as well as against evolving threats and new technologies
- be regularly tested as part of a programme to identify gaps against stated risk tolerance objectives and facilitate improvement of the ICT risk identification, protection, detection and event management
- make use of actionable intelligence to continuously enhance their situational awareness of vulnerabilities to ICT systems, networks and applications and facilitate effective decision making in risk or change management

BUSINESS CONTINUITY PLANNING

PRINCIPLE 11 – BUSINESS CONTINUITY PLANNING: *Banks should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.*

The previous principle in the Review of the Principles for Sound Management of Operational Risk (2014) was titled ‘Business Resilience and Continuity’. However, the 'Resilience' wording has been dropped, and separate principles are to be provided in the Principles for operational resilience paper.

The proposed revisions:

- emphasise the need for board and senior management involvement in reviewing and implementing business continuity plans
- explain that a bank should ground its business continuity policy on scenario analyses of potential disruptions; each disruption scenario should be subject to thresholds or limits for the activation of a business continuity procedure
- state that a bank should periodically review all components of its business continuity policy to ensure that contingency strategies remain consistent with current operations, risks and threats

ROLE OF DISCLOSURE

PRINCIPLE 12 – ROLE OF DISCLOSURE: *A bank’s public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure.*

The proposed changes:

- highlight the importance of ensuring stakeholders are up to date and well-informed about risk management efforts promotes an environment of trust and transparency
- recommend that a bank should disclose its ORMF in a way that allows relevant stakeholders to determine whether the bank identifies, assesses, monitors, and mitigates its operational risk effectively
- suggest that banks should have a formal disclosure policy that is subject to regular and independent review and to approval by the senior management and the board of directors

ROLE OF SUPERVISORS

The revised principles point to greater regulatory scrutiny of bank ORMFs through rising expectations upon national supervisors. Supervisors should regularly assess bank ORMFs by evaluating banks' policies, processes and systems related to operational risk. They should ensure that there are appropriate mechanisms in place allowing them to remain apprised of bank operational risk developments. Supervisory evaluations of operational risk should include all areas described in the principles for the sound management of operational risk.

HOW CAN AVANTAGE REPLY HELP?

Operational risk has matured as a topic since it originally became an integral part of financial institutions' risk management. The Revisions to the PSMOR are expected to contribute to the already-heavy regulatory burden faced by banks. Responding to these challenges, Avantage Reply is supporting risk departments in consolidating existing operational risk management frameworks and developing capability to handle changes.

Avantage Reply provides a number of operational risk services, assisting financial institutions in building and developing their operational risk toolkits, as well as supporting ongoing activities, including:

- Developing comprehensive operational risk management frameworks;
- Implementing methodologies for identifying, assessing, monitoring and reporting operational risk (RCSAs, KRIs, scenario analysis, etc.);
- Quantitative operational risk modelling utilising forward-looking methodologies to determine capital add-ons;
- Achieving compliance with current and forthcoming operational risk regulations; and
- Reviewing and building on outsourcing oversight and governance frameworks.

CONTACTS

Vishwas Khanna, Partner

Vishwas specialises in prudential regulation, risk transformations, programme leadership and new bank authorisations. He is a trusted advisor to the C-Suite and senior management at banks and offers objective, independent advice to his clients to influence strategic decision-making.
vi.khanna@reply.com

Hadrien van der Vaeren, Senior Manager

Hadrien is a senior risk management practitioner specialising in prudential regulation, regulatory reporting, quantitative risk modelling and data and systems implementations. He has experience of delivering complex risk programmes across UK and Europe.
h.vandervaeren@reply.com

Rohan Wilson, Manager

Rohan has significant experience leading regulatory change and risk management projects at key FS clients across challenger and investment banks. He has also supported a European regulator with their internal action plans for resolution of entities.
r.wilson@reply.com

Anastasios Ioannidis, Consultant

Anastasios joined Avantage Reply after graduating from the University of Cambridge with a Master's in Finance and Economics. He has a strong interest in monetary policy and banking regulation.
a.ioannidis@reply.com

AVANTAGE REPLY

Avantage Reply, part of the Reply Group, specialises in Financial Services consulting with a focus on Risk Transformations, Treasury and Capital, Quantitative Modelling and Regulatory Advisory. With offices across Europe, Avantage Reply counts some of the world's most significant financial groups among its clients, including in Investment, Retail and Commercial Banking, Custodian Banking, Insurance and Investment Management.