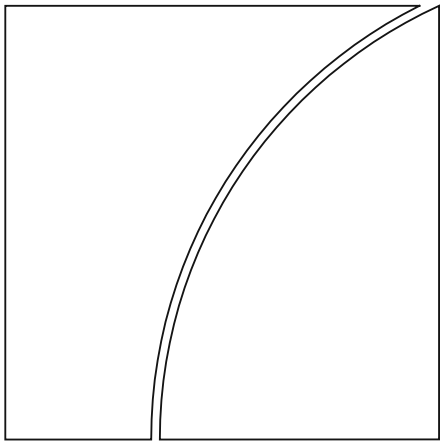
Basel Committee
on Banking Supervision



Revisions to the Principles for the Sound Management of Operational Risk

March 2021

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-468-8 (online)

Contents

Revisions to the Principles for the Sound Management of Operational Risk

1. Introduction

The Basel Committee on Banking Supervision ("the Committee") introduced its Principles for the Sound Management of Operational Risk ("the Principles") in 2003, and subsequently revised them in 2011 to incorporate the lessons from the Great Financial Crisis of 2007–09. In 2014, the Committee conducted a review of the implementation of the Principles.[1] The purpose of this review was to (i) assess the extent to which banks had implemented the Principles; (ii) identify significant gaps in implementation; and (iii) highlight emerging and noteworthy operational risk management practices at banks not currently addressed by the Principles.

The 2014 review identified that several principles had not been adequately implemented, and further guidance would be needed to facilitate their implementation in the following areas:

a) Risk identification and assessment tools, including risk and control self-assessments (RCSAs), key risk indicators, external loss data, business process mapping, comparative analysis, and the monitoring of action plans generated from various operational risk management tools.

b) Change management programmes and processes (and their effective monitoring).

c) Implementation of the three lines of defence, especially by refining the assignment of roles and responsibilities.

d) Board of directors and senior management oversight.

e) Articulation of operational risk appetite and tolerance statements.

f) Risk disclosures.

The Committee also recognised that the 2011 Principles did not sufficiently capture certain important sources of operational risk, such as those arising from information and communication technology (ICT) risk,[2] thus warranting the introduction of a specific principle on ICT risk management. Other revisions were made to ensure consistency with the new operational risk framework in the Basel III reforms.[3]

Recognising the increased potential for significant disruptions to bank operations from pandemics, natural disasters, destructive cyber security incidents or technology failures, the Committee has also developed principles for operational resilience,[4] which reflect several of the principles contained in this document.

[1] BCBS, *Review of the Principles for Sound Management of Operational Risk*, October 2014, www.bis.org/publ/bcbs292.pdf.

[2] Conduct and legal risks (including risks associated with money laundering or terrorist financing) remain important concerns. In this context, financial institutions should continue to improve their ability to manage operational risk.

[3] BCBS, *Basel III: finalising post-crisis reforms*, December 2017, www.bis.org/bcbs/publ/d424.pdf.

[4] "Operational resilience" is defined as the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption. In considering its

2. Components of operational risk management

The Principles in this document for banks cover governance; the risk management environment; information and communication technology; business continuity planning; and the role of disclosure. These elements should not be viewed in isolation; rather, they are integrated components of the operational risk management framework (ORMF) and the overall risk management framework (including operational resilience) of the group.

Through the publication of this document, the Committee desires to promote the effectiveness of operational risk management throughout the banking system. The Committee believes that the Principles reflect sound practices relevant to all banks. Nonetheless, the Committee recommends that banks should take account of the nature, size, complexity and risk profile of their activities when implementing the Principles.

3. Operational risk management

1. Operational risk is defined in the capital framework as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

2. Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk is a fundamental element of a bank's risk management programme. Sound operational risk management is a reflection of the effectiveness of the board of directors and senior management in administering their portfolio of products, activities, processes and systems. Where appropriate, strategic and reputational risks should be considered by banks' operational risk management.

3. Although operational risk management and operational resilience address different goals, they are closely interconnected. An effective operational risk management system and a robust level of operational resilience work together to reduce the frequency and the impact of operational risk events.

4. Sound risk management allows the bank to better understand and mitigate its risk profile. Risk management encompasses identifying risks to the bank; measuring and assessing exposures to those risks (where possible); monitoring exposures and corresponding capital needs on an ongoing basis; taking steps to control or mitigate exposures; and reporting to senior management and the board of directors on the bank's risk exposures and capital positions. Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that the bank's activities are efficient and effective; that information is reliable, timely and complete; and that the bank is compliant with applicable laws and regulations.

5. Sound internal governance forms the foundation of an effective ORMF. Governance of operational risk management has similarities but also differences relative to the management of credit or

operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption. In the context of operational resilience, the Committee defines "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. For more details, refer to BCBS, *Principles for operational resilience,* March 2021, www.bis.org/bcbs/publ/d516.htm.

market risk. Banks' operational risk governance function should be fully integrated into their overall risk management governance structure.

6. Banks commonly rely on three lines of defence: (i) business unit management; [5] (ii) an independent corporate operational risk management function (CORF);[6] and (iii) independent assurance.[7] Depending on the bank's nature, size and complexity, and the risk profile of a bank's activities, the degree of formality of how these three lines of defence are implemented will vary.

7. Banks should ensure that each line of defence:

a) is adequately resourced in terms of budget, tools and staff;

b) has clearly defined roles and responsibilities;

c) is continuously and adequately trained;

d) promotes a sound risk management culture across the organisation; and

e) communicates with the other lines of defence to reinforce the ORMF.

If in one business unit there are functions of both the first and second line of defence, then banks should document and distinguish the responsibilities of such functions in the first and second line of defence, emphasising the independence of the second line of defence.

8. The Committee has highlighted that, despite the three lines of defence model being widely adopted by banks, confusion around roles and responsibilities sometimes hampers its effectiveness.[8] Thus, the review of the Principles is also the opportunity to stress that this model should be adequately and proportionally used by financial institutions to manage every kind of operational risk subcategory, including ICT risk.

9. In industry practice, the first line of defence is business unit management. Sound operational risk governance recognises that business unit management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable. Banks should have a policy that defines clear roles and responsibilities in relevant business units.[9] The responsibilities of an effective first line of defence in promoting a sound operational risk management culture should include:

a) identifying and assessing the materiality of operational risks inherent in their respective business units through the use of operational risk management tools;

[5] The term "business unit" is meant broadly to include all associated support, corporate and/or shared service functions, eg Finance, Human Resources, and Operations and Technology. Risk Management and Internal Audit are not included unless otherwise specifically indicated.

[6] In addition to an independent Operational Risk Management function, the second line of defense also typically includes a Compliance function.

[7] Independent assurance includes verification and validation: verification of the ORMF is done on a periodic basis and is typically conducted by the bank's internal and/or external audit, but may involve other suitably qualified independent third parties from external sources. Verification activities test the effectiveness of the overall ORMF, consistent with policies approved by the board of directors, and also test validation processes to ensure they are independent and implemented in a manner consistent with established bank policies. Validation ensures that the quantification systems used by the bank are sufficiently robust and provide assurance of the integrity of inputs, assumptions, methodologies, processes and outputs. Validation is critical for a well functioning ORMF.

[8] See BCBS, *Cyber resilience: range of practices*, December 2018, https://www.bis.org/bcbs/publ/d454.pdf,

[9] In complex banking structures, "relevant business units" are likely to include support functions such as information systems departments.

b) establishing appropriate controls to mitigate inherent operational risks, and assessing the design and effectiveness of these controls through the use of the operational risk management tools;

c) reporting whether the business units lack adequate resources, tools and training to ensure identification and assessment of operational risks;

d) monitoring and reporting the business units' operational risk profiles,[10] and ensuring their adherence to the established operational risk appetite and tolerance statement; and

e) reporting residual operational risks not mitigated by controls, including operational loss events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances.

10. A functionally independent CORF is typically the second line of defence. The responsibilities of an effective second line of defence should include:

a) developing an independent view regarding business units' (i) identified material operational risks, (ii) design and effectiveness of key controls, and (iii) risk tolerance;

b) challenging the relevance and consistency of the business unit's implementation of the operational risk management tools, measurement activities and reporting systems, and providing evidence of this effective challenge;

c) developing and maintaining operational risk management and measurement policies, standards and guidelines;

d) reviewing and contributing to the monitoring and reporting of the operational risk profile; and

e) designing and providing operational risk training and instilling risk awareness.

11. The degree of independence of the CORF may differ among banks. At small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF should have a reporting structure independent of the risk-generating business units and be responsible for the design, maintenance and ongoing development of the ORMF within the bank. The CORF typically engages relevant corporate control groups (eg Compliance, Legal, Finance and IT) to support its assessment of the operational risks and controls. Banks should have a policy which defines clear roles and responsibilities of the CORF, reflective of the size and complexity of the organisation.

12. The third line of defence provides independent assurance to the board of the appropriateness of the bank's ORMF. This function's staff should not be involved in the development, implementation and operation of operational risk management processes by the other two lines of defence. The third line of defence reviews generally are conducted by the bank's internal and/or external audit, but may also involve other suitably qualified independent third parties. The scope and frequency of reviews should be sufficient to cover all activities and legal entities of a bank. An effective independent review should:

a) review the design and implementation of the operational risk management systems and associated governance processes through the first and second lines of defence (including the independence of the second line of defence);

b) review validation processes to ensure they are independent and implemented in a manner consistent with established bank policies;

[10] Operational risk profiles describe the operational risk exposures and control environment assessments of business units and consider the range of potential impacts that could arise from estimates of expected to severe losses. Profiles generally provide management and the board of directors with a representation of operational risk exposures at a level which supports their decision-making and oversight responsibilities.

c) ensure that the quantification systems used by the bank are sufficiently robust as (i) they provide assurance of the integrity of inputs, assumptions, processes and methodology and (ii) result in assessments of operational risk that credibly reflect the operational risk profile of the bank;

d) ensure that business units' management promptly, accurately and adequately responds to the issues raised, and regularly reports to the board of directors or its relevant committees on pending and closed issues; and

e) opine on the overall appropriateness and adequacy of the ORMF and the associated governance processes across the bank. Beyond checking compliance with policies and procedures approved by the board of directors, the independent review should also assess whether the ORMF meets organisational needs and expectations (such as respect of the corporate risk appetite and tolerance, and adjustment of the framework to changing operating circumstances) and complies with statutory and legislative provisions, contractual arrangements, internal rules and ethical conduct.

13. Because operational risk management is evolving and the business environment is constantly changing, senior management should ensure that the ORMF's policies, processes and systems remain sufficiently robust to manage and ensure that operational losses are adequately addressed in a timely manner. Improvements in operational risk management depend heavily on senior management's willingness to be proactive and also act promptly and appropriately to address operational risk managers' concerns.

4. Principles for the sound management of operational risk

Principle 1: The board of directors should take the lead in establishing a strong risk management culture, implemented by senior management.[11] *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.*

14. Banks with a strong culture of risk management and ethical business practices are less likely to experience damaging operational risk events and are better placed to effectively deal with those events that occur. The actions of the board of directors and senior management as well as the bank's risk management policies, processes and systems provide the foundation for a sound risk management culture.

15. The board of directors should establish a code of conduct or an ethics policy to address conduct risk. This code or policy should be applicable to both staff and board members, set clear expectations for integrity and ethical values of the highest standard, identify acceptable business practices, and prohibit

[11] This paper refers to a management structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries regarding the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms "board of directors" and "senior management" are used in this paper not to identify legal constructs but rather to label two decision-making functions within a bank.

conflicts of interest or the inappropriate provision of financial services (whether wilful or negligent). The code or policy should be regularly reviewed and approved by the board of directors and attested by employees; its implementation should be overseen by a senior ethics committee, or another board-level committee, and should be publicly available (eg on the bank's website). A separate code of conduct may be established for specific positions in the bank (eg treasury dealers, senior management).

16. Management should set clear expectations and accountabilities to ensure bank staff understands their roles and responsibilities for risk management, as well as their authority to act.

17. Compensation policies should be aligned to the bank's statement of risk appetite and tolerance as well as overall safety and soundness, and appropriately balance risk and reward.[12]

18. Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organisation, such as heads of business units, heads of internal controls and senior managers. Training provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

19. Strong and consistent board of directors and senior management support for operational risk management and ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, and training programmes.

Principle 2: Banks should develop, implement and maintain an operational risk management framework 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.

20. The board of directors and bank management should understand the nature and complexity of the risks inherent in the portfolio of bank products, services, activities, and systems, which is a fundamental premise of sound risk management. This is particularly important for operational risk, given operational risk is inherent in all business products, activities, processes and systems.

21. 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. 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. In addition, results of the bank's operational risk assessment should be incorporated into the bank's overall business strategy development process.

22. The ORMF should be comprehensively and appropriately documented in board of directors approved policies and include definitions of operational risk and operational loss. Banks that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their ORMF.

23. ORMF documentation should clearly:

a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities, and the mandates and membership of the operational risk governance committees;

b) reference the relevant operational risk management policies and procedures;

[12] See also BCBS, *Report on the range of methodologies for the risk and performance alignment of remuneration,* May 2011*;* Financial Stability Forum, *Principles for sound compensation practices*, April 2009; Financial Stability Board, *FSB principles for sound compensation practices – implementation standards*, September 2009; and the Financial Stability Board's toolkit *Strengthening Governance Frameworks to Mitigate Misconduct Risk*, April 2018.

c) describe the tools for risk and control identification and assessment and the role and responsibilities of the three lines of defence in using them;

d) describe the bank's accepted operational risk appetite and tolerance; the thresholds, material activity triggers or limits for inherent and residual risk; and the approved risk mitigation strategies and instruments;

e) describe the bank's approach to ensure controls are designed, implemented and operating effectively;

f) describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

g) inventory risks and controls implemented by all business units (eg in a control library);

h) establish risk reporting and management information systems (MIS) producing timely, and accurate data;

i) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives across all business units.[13] The taxonomy can distinguish operational risk exposures by event types, causes, materiality and business units where they occur; it can also flag those operational exposures that partially or entirely represent legal, conduct, model and ICT (including cyber) risks as well as exposures in the credit or market risk boundary;

j) provide for appropriate independent review and challenge of the outcomes of the risk management process; and

k) require the policies to be reviewed and revised as appropriate based on continued assessment of the quality of the control environment addressing internal and external environmental changes or whenever a material change in the operational risk profile of the bank occurs.

Governance[14]

Board of directors

Principle 3: The board of directors should approve and periodically review the operational risk management framework, and ensure that senior management implements the policies, processes and systems of the operational risk management framework effectively at all decision levels.

24. The board of directors should:

a) establish a risk management culture and ensure that the bank has adequate processes for understanding the nature and scope of the operational risk inherent in the bank's current and planned strategies and activities;

b) ensure that the operational risk management processes are subject to comprehensive and dynamic oversight and are fully integrated into, or coordinated with, the overall framework for managing all risks across the enterprise;

[13] An inconsistent taxonomy of operational risk terms may increase the likelihood of failure to identify and categorise risks, or failure to allocate responsibility for the assessment, monitoring, control and mitigation of risks. For the particular case of cyber risk, the Financial Stability Board's Cyber Lexicon, published in November 2018, should be used as a starting point.

[14] See also BCBS, *Principles for enhancing corporate governance*, October 2010.

c) provide senior management with clear guidance regarding the principles underlying the ORMF, and approve the corresponding policies developed by senior management to align with these principles;

d) regularly review and evaluate the effectiveness of, and approve the ORMF to ensure the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (eg changing business volumes);

e) ensure that the bank's ORMF is subject to effective independent review by a third line of defence (audit or other appropriately trained independent third parties from external sources); and

f) ensure that, as best practice evolves, management is availing themselves of these advances.[15]

25. Strong internal controls are a critical aspect of operational risk management. The board of directors should establish clear lines of management responsibility and accountability for implementing a strong control environment. Controls should be regularly reviewed, monitored, and tested to ensure ongoing effectiveness. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business units and support functions.

Principle 4: The board of directors should approve and periodically review a risk appetite and tolerance statement[16] *for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume.*

26. The risk appetite and tolerance statement for operational risk should be developed under the authority of the board of directors and linked to the bank's short- and long-term strategic and financial plans. Taking into account the interests of the bank's customers and shareholders as well as regulatory requirements, an effective risk appetite and tolerance statement should:

a) be easy to communicate and therefore easy for all stakeholders to understand;

b) include key background information and assumptions that informed the bank's business plans at the time it was approved;

c) include statements that clearly articulate the motivations for taking on or avoiding certain types of risk, and establish boundaries or indicators (which may be quantitative or not) to enable monitoring of these risks;

d) ensure that the strategy and risk limits of business units and legal entities, as relevant, align with the bank-wide risk appetite statement; and

e) be forward-looking and, where applicable, subject to scenario and stress testing to ensure that the bank understands what events might push it outside its risk appetite and tolerance statement.

27. The board of directors should approve and regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review should consider current and expected changes in the external environment (including the regulatory context across all jurisdictions where the institution provides services); ongoing or forthcoming material increases in business or activity

[15] See the Committee's 2006 *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*; paragraph 718(xci).

[16] See the Committee's 2015 *Corporate governance guidelines*, which use the FSB's 2013 *Principles for an effective risk appetite framework* definition of risk appetite: the aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan. "Risk tolerance" is the variation around the prescribed risk appetite that the bank is willing to tolerate.

volumes; the quality of the control environment; the effectiveness of risk management or mitigation strategies; loss experience; and the frequency, volume or nature of limit breaches. The board of directors should monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

Senior management

Principle 5: 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.

28. Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue resolution processes. These should include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks should be able to demonstrate that the three-lines-of-defence approach is operating satisfactorily and to explain how the board of directors, independent audit committee of the board, and senior management ensure that this approach is implemented and operating in an appropriate manner.

29. Senior management should translate the ORMF approved by the board of directors into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure the necessary resources are available to manage operational risk in line with the bank's risk appetite and tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.

30. Senior management should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance risk transfer and other third-party arrangements (including outsourcing). Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

31. The managers of the CORF should be of sufficient stature within the bank to perform their duties effectively, ideally evidenced by a title that is commensurate with other risk management functions such as credit, market and liquidity risk.

32. Senior management should ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee.

33. A bank's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration:

a) Committee structure – Sound industry practice is for larger and more complex organisations with a central group function and separate business units to utilise a board-created enterprise-level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise-level risk committee may receive input from operational risk committees by country, business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee.

b) Committee composition – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include members with a variety of expertise, which should cover expertise in business activities, financial activities, legal, technological and regulatory matters, and independent risk management.[17]

c) Committee operation – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

Risk management environment

Identification and assessment

Principle 6: 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.

34. Risk identification and assessment are fundamental characteristics of an effective operational risk management system, and directly contribute to operational resilience capabilities. Effective risk identification considers both internal factors and external factors. Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively.

35. Examples of tools used for identifying and assessing operational risk are:[18]

a) Event management – When banks experience an operational risk event, the process of identification, analysis, end-to-end management and reporting of the event follows a pre-determined set of protocols. A sound event management approach typically includes analysis of events to identify new operational risks, understanding the underlying causes and control weaknesses, and formulating an appropriate response to prevent recurrence of similar events. This information is an input to the self-assessment and, in particular, to the assessment of control effectiveness.

b) Operational risk event data – Banks often maintain a comprehensive operational risk event dataset that collects all material events experienced by the bank and serves as basis for operational risk assessments. The event dataset typically includes internal loss data, near misses, and, when feasible, external operational loss event data (as external data is informative of risks that common across the industry). Event data is typically classified according to a taxonomy defined in the ORMF policies and consistently applied across the bank. Event data typically include the date of the event (occurrence date, discovery date and accounting date) and, in the case of loss events, financial impact. When other root cause information for events is available, ideally it can also be included in the operational risk dataset. When feasible, banks are encouraged to also seek to gather external operational risk event data and use this data in their internal analysis, as it is often informative of risks that are common across the industry.

c) Self-assessments – Banks often perform self-assessments of their operational risks and controls on various different levels. The assessments typically evaluate inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk

[17] See the Committee's 2015 *Corporate governance principles for banks* for additional requirements on the Committee composition.

[18] This list is not comprehensive and does not reflect the full diversity of sophistication of possible analyses. It should be seen as indicative (and not limitative).

exposure after controls are considered) and contain both quantitative and qualitative elements. The qualitative element reflects consideration of both the likelihood and consequence of the risk event in the bank's determination of its inherent and residual risk ratings. The assessments may utilise business process mapping to identify key steps in business processes, activities, and organisational functions, as well as the associated risks and areas of control weakness.The assessments contain sufficiently detailed information on the business environment, operational risks, underlying causes, controls and evaluation of control effectiveness to enable an independent reviewer to determine how the bank reached its ratings. A risk register can be maintained to collate this information to form a meaningful view of the overall effectiveness of controls and facilitate oversight by senior management, risk committees, and the board of directors.

d) Control monitoring and assurance framework – Incorporating an appropriate control monitoring and assurance framework facilitates a structured approach to the evaluation, review and ongoing monitoring and testing of key controls. The analysis of controls ensures these are suitably designed for the identified risks and operating effectively. The analysis should also consider the sufficiency of control coverage, including adequate prevention, detection and response strategies. The control monitoring and testing should be appropriate for the different operational risks and key controls across business areas.

e) Metrics – Using operational risk event data and risk and control assessments, banks often develop metrics to assess and monitor their operational risk exposure. These metrics may be simple indicators, such as event counts, or result from more sophisticated exposure models when appropriate. Metrics provide early warning information to monitor ongoing performance of the business and the control environment, and to report the operational risk profile. Effective metrics clearly link to the associated operational risks and controls. Monitoring metrics and related trends through time against agreed thresholds or limits provides valuable information for risk management and reporting purposes.

f) Scenario analysis – Scenario analysis is a method to identify, analyse and measure a range of scenarios, including low probability and high severity events, some of which could result in severe operational risk losses. Scenario analysis typically involves workshop meetings of subject matter experts including senior management, business management and senior operational risk staff and other functional areas such as compliance, human resources and IT risk management, to develop and analyse the drivers and range of consequences of potential events. Inputs to the scenario analysis would typically include relevant internal and external loss data, information from self-assessments, the control monitoring and assurance framework, forward-looking metrics, root-cause analyses and the process framework, where used. The scenario analysis process could be used to develop a range of consequences of potential events, including impact assessments for risk management purposes, supplementing other tools based on historical data or current risk assessments. It could also be integrated with disaster recovery and business continuity plans, for use within testing of operational resilience. Given the subjectivity of the scenario process, a robust governance framework and independent review are important to ensure the integrity and consistency of the process.

g) Benchmarking and comparative analysis – Benchmarking and comparative analysis are comparisons of the outcomes of different risk measurement and management tools deployed within the bank, as well as comparisons of metrics from the bank to other firms in the industry. Such comparisons can be performed to enhance understanding of the bank's operational risk profile. For example, comparing the frequency and severity of internal losses with self-assessments can help the bank determine whether its self-assessment processes are functioning effectively. Scenario data can be compared to internal and external loss data to gain a better understanding of the severity of the bank's exposure to potential risk events.

36. Banks should ensure that the operational risk assessment tools' outputs are:

a) based on accurate data, whose integrity is ensured by strong governance and robust verification and validation procedures;

b) adequately taken into account in the internal pricing and performance measurement mechanisms as well as for business opportunities assessments; and

c) subject to CORF-monitored action plans or remediation plans when necessary.

37. These operational risk assessment tools can also directly contribute to a bank's operational resilience approach, in particular event management, self assessment and scenario analysis procedures, as they allow banks to identify and monitor threats and vulnerabilities to their critical operations. Banks should use the outputs of these tools to improve their operational resilience controls and procedures, as identified in the Committee's *Principles for operational resilience*.[19]

Principle 7: Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and adequately articulated between the relevant lines of defence.

38. In general, a bank's operational risk exposure evolves when a bank initiates change, such as engaging in new activities or developing new products or services; entering into unfamiliar markets or jurisdictions; implementing new or modifying business processes or technology systems; and/or engaging in businesses that are geographically distant from the head office. Change management should assess the evolution of associated risks across time, from inception to termination (eg throughout the full life cycle of a product). [20]

39. A bank should have 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 clearly allocate roles and responsibilities in accordance with the three-lines-of-defence model, in particular:

a) The first line of defence should perform operational risk and control assessments of new products, activities, processes and systems, including the identification and evaluation of the required change through the decision-making and planning phases to the implementation and post-implementation review.

b) The second line of defence (CORF) should challenge the operational risk and control assessments of first line of defence, as well as monitor the implementation of appropriate controls or remediation actions. CORF should cover all phases of this process. In addition, CORF should ensure that all relevant control groups (eg finance, compliance, legal, business, ICT, risk management) are involved as appropriate.

40. A bank should have policies and procedures for the review and approval of new products, activities, processes and systems. The review and approval process should consider:

[19] These controls and procedures should be consistent with and conducted alongside the identification of threats and vulnerabilities as part of a bank's operational resilience approach as articulated in Principle 2 in the Committee's *Principles for operational resilience,* March 2021.

[20] The life cycle of a product or service encompasses various stages from the development, ongoing changes, grandfathering and closure. Indeed, the level of risk may escalate for example when new products, activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations.

a) Inherent risks – including legal, ICT and model risks – in the launch of new products, services, activities, and operations in unfamiliar markets, and in the implementation of new processes, people and systems (especially when outsourced).

b) Changes to the bank's operational risk profile, appetite and tolerance, including changes to the risk of existing products or activities.

c) The necessary controls, risk management processes, and risk mitigation strategies.

d) The residual risk.

e) Changes to relevant risk thresholds or limits.

f) The procedures and metrics to assess, monitor, and manage the risk of new products, services, activities, markets, jurisdictions, processes and systems.

41. The review and approval process should include ensuring that appropriate investment has been made for human resources and technology infrastructure before changes are introduced. Changes should be monitored, during and after their implementation, to identify any material differences to the expected operational risk profile and manage any unexpected risks.

42. 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.

Monitoring and reporting

Principle 8: 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.

43. A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business units and products. To this end, 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. Reports should be manageable in scope and volume by providing an outlook on the bank's operational risk profile and adherence to the operational risk appetite and tolerance statement; effective decision-making is impeded by both excessive amounts and paucity of data.

44. Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions.[21] The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. The results of monitoring activities should be included in regular management and board reports, as should assessments of the ORMF performed by the internal/external audit and/or risk management functions. Reports generated by or for supervisory authorities should also be reported internally to senior management and the board of directors, where appropriate.

45. Operational risk reports should describe the operational risk profile of the bank by providing internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational risk reports should include:

[21] Reporting should be consistent with the Committee's *Principles for effective risk data aggregation and risk reporting* (https://www.bis.org/publ/bcbs239.pdf).

a) Breaches of the bank's risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements.

b) A discussion and assessment of key and emerging risks.

c) Details of recent significant internal operational risk events and losses (including root cause analysis).

d) Relevant external events or regulatory changes and any potential impact on the bank.

46. Data capture and risk reporting processes should be analysed periodically with the goal of enhancing risk management performance as well as advancing risk management policies, procedures and practices.

Control and mitigation

Principle 9: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

47. Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme consists of four components that are integral to the risk management process: risk assessment, control activities, information and communication, and monitoring activities.[22]

48. Control processes and procedures should include a system for ensuring compliance with policies, regulations and laws. Examples of principle elements of a policy compliance assessment are:

a) Top-level reviews of progress towards stated objectives.

b) Verification of compliance with management controls.

c) Review of the treatment and resolution of instances of non-compliance.

d) Evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management.

e) Tracking of reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy, regulations and laws.

49. Controls processes and procedures should address how the bank ensures operational resilience is maintained in both normal circumstances and in the event of disruption, reflecting respective functions' due diligence, consistent with the bank's operational resilience approach.

50. An effective control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team, without dual controls (eg a process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information) or other countermeasures, may result in concealment of losses, errors or other inappropriate actions. Therefore, areas where conflicts of interest may arise should be identified, minimised, and be subject to careful independent monitoring and review.

51. In addition to segregation of duties and dual controls, banks should ensure that other traditional internal controls are in place, as appropriate, to address operational risk. Examples of these controls are:

a) Clearly established authorities and/or processes for approval.

[22] The Committee's paper *Framework for Internal Control Systems in Banking Organisations*, September 1998, discusses internal controls in greater detail.

b) Close monitoring of adherence to assigned risk thresholds or limits.

c) Safeguards for access to, and use of, bank assets and records.

d) Appropriateness of staffing level and training to maintain technical expertise.

e) Ongoing processes to identify business units or products where returns appear to be out of line with reasonable expectations.[23]

f) Regular verification and reconciliation of transactions and accounts.

g) Vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

52. Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management programmes.

53. The use of technology related products, activities, processes and delivery channels exposes a bank to operational risk and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks along the same precepts as operational risk management.

54. While recourse to entities such as, but not limited to third-party service providers can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board of directors 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. Amongst others, the concentration of risk and the complexity of outsourcing should be taken into account. Third-party risk policies (as a part of the ORMF's policies) and risk management activities[24] should encompass:

a) Procedures for determining whether and how activities can be outsourced.

b) Processes for conducting due diligence in the selection of potential service providers.

c) Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights.

d) Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider.

e) Establishment of an effective control environment at the bank and the service provider, that should include a register of outsourced activities and metrics and reporting to faciliate oversight of the service provider.

f) Development of viable contingency plans.

g) Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

h) Banks' supervisory and resolution authorities' access to third parties.

[23] For example, where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach.

[24] These risk policies and risk management activities should be consistent with and conducted alongside the critical operations management and dependency management for operational resilience. Basel Committee on Banking Supervision, *Principles for operational resilience*, March 2021.

55. 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. The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management programme. While the specific insurance or risk transfer needs of a bank should be determined on an individual basis, many jurisdictions have regulatory requirements that must be considered.

56. Because risk transfer is an imperfect substitute for sound controls and risk management programmes, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors – or specific legal risk exposure - can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (eg counterparty risk).

57. Banks should have unified classification, methodology, and procedures of operational risk management established by the CORF.

Information and communication technology

Principle 10: Banks should implement a robust ICT[25] risk management programme in alignment with their operational risk management framework.

58. Effective ICT performance and security are paramount for a bank to conduct its business properly. The appropriate use and implementation of sound ICT risk management contributes to the effectiveness of the control environment and is fundamental to the achievement of a bank's strategic objectives. A bank's ICT risk assessment should ensure that its ICT fully supports and facilitates its operations. ICT risk management should reduce a bank's operational risk exposure to direct losses, legal claims, reputational damage, ICT disruption and misuse of technology in alignment with its risk appetite and tolerance statement.

59. ICT risk management includes:

a) ICT risk identification and assessment.

b) ICT risk mitigation measures consistent with the assessed risk level (eg cybersecurity, response and recovery programmes, ICT change management processes, ICT incident management processes, including relevant information transmission to users on a timely basis).

c) Monitoring of these mitigation measures (including regular tests).

60. To ensure data and systems' confidentiality, integrity and availability, the board of directors should regularly oversee the effectiveness of the bank's ICT risk management and senior management should routinely evaluate the design, implementation and effectiveness of the bank's ICT risk management. This requires regular alignment of the business, risk management and ICT strategies to be consistent with the bank's risk appetite and tolerance statement as well as with privacy and other applicable laws. Banks should continuously monitor its ICT and regularly report to senior management on ICT risks, controls and events.

61. ICT risk management together with complementing processes set by the banks should:

[25] "Information and communication technology" refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environments.

a) be reviewed on a regular basis for completeness against relevant industry standards and best practices as well as against evolving threats (eg cyber) and evolving or new technologies;

b) 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; and

c) 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.

62. Banks should develop approaches to ICT readiness for stressed scenarios from disruptive external events, such as the need to facilitate the implementation of wide-scale remote-access, rapid deployment of physical assets and/or significant expansion of bandwidth to support remote user connections and customer data protection. Banks should ensure that:

a) appropriate risk mitigation strategies are developed for potential risks associated with a disruption or compromise of ICT systems, networks and applications. Banks should evaluate whether the risks, taken together with these strategies, fall within the bank's risk appetite and risk tolerance;

b) well defined processes for the management of privileged users and application development are in place; and

c) regular updates are made to ICT including cyber security in order to maintain an appropriate security posture.

Business continuity planning

Principle 11: 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.[26] *Business continuity plans should be linked to the bank's operational risk management framework.*

63. Sound and effective governance of banks' business continuity policy[27] requires:

a) Regular review and approval by the board of directors.

b) The strong involvement of the senior management and business units leaders in its implementation.

c) The commitment of the first and second lines of defence to its design.

d) Regular review by the third line of defence.

64. Banks should prepare forward-looking business continuity plans (BCP) with scenario analyses associated with relevant impact assessments and recovery procedures:

a) A bank should ground its business continuity policy on scenario analyses of potential disruptions that identify and categorise critical business operations and key internal or external

[26] The Committee's paper *High-level principles for business continuity*, August 2006, discusses sound continuity principles in greater detail.

[27] Business continuity planning should be consistent with and conducted alongside the business continuity planning and testing of critical operations as specified in the principles for operational resilience. BCBS, *Principles for operational resilience,* March 2021.

dependencies. In doing so, banks should cover all their business units as well as critical providers and major third parties (eg central banks, clearing house).

b) Each scenario should be subject to a quantitative and qualitative impact assessment or business impact analysis (BIA) with regards to its financial, operational, legal and reputational consequences.

c) Disruption scenarios should be subject to thresholds or limits (such as maximum tolerable outage) for the activation of a business continuity procedure. The procedure should address resumption aspects, set recovery time objectives (RTO) and recovery point objectives (RPO) as well as communication guidelines for informing management, employees, regulatory authorities, customers, suppliers, and – where appropriate – civil authorities.

65. A bank should periodically review its business continuity plans and policies to ensure that contingency strategies remain consistent with current operations, risks and threats. Training and awareness programmes should be customised based on specific roles to ensure that staff can effectively execute contingency plans. Business continuity procedures should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in business continuity testing with key service providers. Results of formal testing and review activities should be reported to senior management and the board of directors.

Role of disclosure

Principle 12: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure.

66. A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice.

67. 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).[28,29] A bank should disclose its ORMF in a manner that allows stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

68. Banks should have a formal disclosure policy that is subject to regular and independent review and approval by the senior management and the board of directors. The policy should address the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures and disclosure policy.

Role of supervisors

69. Supervisors should regularly assess banks' ORMF by evaluating banks' policies, processes and systems related to operational risk. Supervisors should ensure that there are appropriate mechanisms in place allowing them to remain apprised of banks' operational risk developments.

[28] Internationally active banks are required to comply with the Basel III Pillar 3 operational risk disclosure requirements.

[29] The recommendation to disclose significant operational loss events does not include disclosure of confidential and proprietary information, including information about legal reserves.

70. Supervisory evaluations of operational risk should include all areas described in the Principles for the sound management of operational risk. Where banks are part of a financial group, supervisors should ensure that there are processes in place to ensure that operational risk is managed in an appropriate and integrated manner across the group. In assessing banks' ORMF, cooperation and exchange of information with other supervisors, in accordance with established procedures, may be necessary.[30] In certain circumstances, supervisors may choose to use external auditors in these assessment processes.[31]

71. Supervisors should take steps to ensure that banks address deficiencies identified through the supervisory review of banks' ORMF. Supervisors should use the tools most suited to the particular circumstances of banks and their operating environment. To ensure that supervisors receive current information on operational risk, supervisors may wish to establish reporting mechanisms directly with banks and external auditors (eg internal bank management reports on operational risk could be made routinely available to supervisors).

72. Supervisors should encourage banks' ongoing internal development efforts by monitoring, comparing and evaluating banks' recent improvements and plans for prospective developments.

[30] Refer to the Committee's papers *High-level principles for the cross-border implementation of the New Accord*, August 2003, and *Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA)*, November 2007.

[31] For further discussion, see the Committee's paper *The relationship between banking supervisors and bank's external auditors*, January 2002.