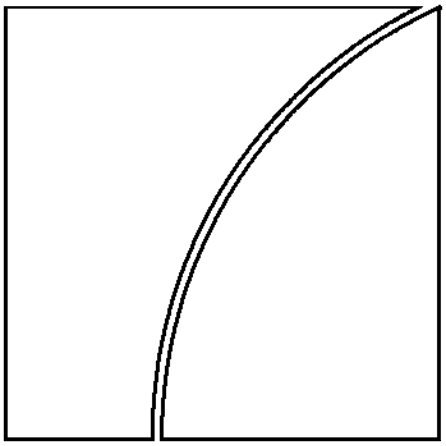
Basel Committee
on Banking Supervision



Principles for the Sound Management of Operational Risk

June 2011

BANK FOR INTERNATIONAL SETTLEMENTS

Copies of publications are available from:

Bank for International Settlements
Communications
CH-4002 Basel, Switzerland

E-mail: publications@bis.org

Fax: +41 61 280 9100 and +41 61 280 8100

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

ISBN 92-9131-857-4 (print)
ISBN 92-9197-857-4 (online)

Members of the SIG Operational Risk Subgroup

Chairman: Mitsutoshi Adachi, Bank of Japan

Australian Prudential Regulation Authority	Michael Booth
National Bank of Belgium	Jos Meuleman
Banco Central do Brasil, Brazil	Wagner Almeida
Office of the Superintendent of Financial Institutions, Canada	James Dennison Aina Liepins
China Banking Regulatory Commission	Meng Luo
Banque de France	Jean-Luc Quémard
Deutsche Bundesbank, Germany	Marcus Haas
Federal Financial Supervisory Authority (BaFin), Germany	Frank Corleis
Reserve Bank of India	Rajinder Kumar
Bank of Italy	Marco Moscadelli
Bank of Japan	Madoka Miyamura
Financial Services Agency, Japan	Tsuyoshi Nagafuji
Surveillance Commission for the Financial Sector, Luxembourg	Didier Bergamo
Netherlands Bank	Claudia Zapp
Polish Financial Supervision Authority	Grazyna Szwajkowska
Central Bank of the Russian Federation	Irina Yakimova
South African Reserve Bank	Jan van Zyl
Bank of Spain	María Ángeles Nieto
Finansinspektionen, Sweden	Agnieszka Arshamian
Swiss Financial Market Supervisory Authority	Paul Harpes
Financial Services Authority, United Kingdom	Andrew Sheen Khim Murphy
Federal Deposit Insurance Corporation, United States	Alfred Seivold
Federal Reserve Board, United States	Adrienne Townes Haden Kenneth G. Fulton
Federal Reserve Bank of Boston, United States	Patrick de Fontnouvelle
Federal Reserve Bank of New York, United States	Ronald Stroz
Office of the Comptroller of the Currency, United States	Carolyn DuChene Maurice Harris
Office of Thrift Supervision, United States	Eric Hirschhorn
Financial Stability Institute	Amarendra Mohan
Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements	Andrew Willis

Contents

Principles for the Sound Management of Operational Risk and the Role of Supervision

Preface

1. In the *Sound Practices for the Management and Supervision of Operational Risk* (Sound Practices), published in February 2003, the Basel Committee on Banking Supervision (Committee) articulated a framework of principles for the industry and supervisors. Subsequently, in the 2006 *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version* (commonly referred to as "Basel II"), the Committee anticipated that industry sound practice would continue to evolve.[1] Since then, banks and supervisors have expanded their knowledge and experience in implementing operational risk management frameworks (Framework). Loss data collection exercises, quantitative impact studies, and range of practice reviews covering governance, data and modelling issues have also contributed to industry and supervisory knowledge and the emergence of sound industry practice.

2. In response to these changes, the Committee has determined that the 2003 Sound Practices paper should be updated to reflect the enhanced sound operational risk management practices now in use by the industry. This document – *Principles for the Sound Management of Operational Risk and the Role of Supervision* – incorporates the evolution of sound practice and details eleven principles of sound operational risk management covering (1) governance, (2) risk management environment and (3) the role of disclosure. By publishing an updated paper, the Committee enhances the 2003 sound practices framework with specific principles for the management of operational risk that are consistent with sound industry practice. These principles have been developed through the ongoing exchange of ideas between supervisors and industry since 2003. *Principles for the Sound Management of Operational Risk and the Role of Supervision* replaces the 2003 Sound Practices and becomes the document that is referenced in paragraph 651 of Basel II.

3. *A Framework for Internal Control Systems in Banking Organisations* (Basel Committee, September 1998) underpins the Committee's current work in the field of operational risk. *The Core Principles for Effective Banking Supervision* (Basel Committee, October 2006) and the *Core Principles Methodology* (Committee, October 2006), both for supervisors, and the principles identified by the Committee in the second pillar (supervisory review process) of Basel II are also important reference tools that banks should consider when designing operational risk policies, processes and risk management systems.

4. Supervisors will continue to encourage banks "to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices".[2] Consequently, while this paper articulates principles from emerging sound industry practice, supervisors expect banks to

---

[1] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, Section V (Operational Risk), paragraph 646, Basel, June 2006.

[2] BCBS (2006), paragraph 646.

continuously improve their approaches to operational risk management. In addition, this paper addresses key elements of a bank's Framework. These elements should not be viewed in isolation but should be integrated components of the overall framework for managing operational risk across the enterprise.

5. The Committee believes that the principles outlined in this paper establish sound practices relevant to all banks. The Committee intends that when implementing these principles, a bank will take account of the nature, size, complexity and risk profile of its activities.

Role of Supervisors

6. Supervisors conduct, directly or indirectly, regular independent evaluations of a bank's policies, processes and systems related to operational risk as part of the assessment of the Framework. Supervisors ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at a bank**.**

7. Supervisory evaluations of operational risk include all the areas described in the principles for the management of operational risk. Supervisors also seek to ensure that, where banks are part of a financial group, there are processes and procedures in place to ensure that operational risk is managed in an appropriate and integrated manner across the group. In performing this assessment, cooperation and exchange of information with other supervisors, in accordance with established procedures, may be necessary.[3] Some supervisors may choose to use external auditors in these assessment processes.[4]

8. Deficiencies identified during the supervisory review may be addressed through a range of actions. Supervisors use the tools most suited to the particular circumstances of the bank and its operating environment. In order that supervisors receive current information on operational risk, they 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).

9. Supervisors continue to take an active role in encouraging ongoing internal development efforts by monitoring and evaluating a bank's recent improvements and plans for prospective developments. These efforts can then be compared with those of other banks to provide the bank with useful feedback on the status of its own work. Further, to the extent that there are identified reasons why certain development efforts have proven ineffective, such information could be provided in general terms to assist in the planning process.

---

[3] 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.

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

Principles for the management of operational risk

10. Operational risk[5] is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management programme. As a result, sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems. The Committee, through the publication of this paper, desires to promote and enhance the effectiveness of operational risk management throughout the banking system.

11. Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board 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 bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each.

12. Sound internal governance forms the foundation of an effective operational risk management Framework. Although internal governance issues related to the management of operational risk are not unlike those encountered in the management of credit or market risk operational risk management challenges may differ from those in other risk areas.

13. The Committee is seeing sound operational risk governance practices adopted in an increasing number of banks. Common industry practice for sound operational risk governance often relies on three lines of defence – (i) business line management, (ii) an independent corporate operational risk management function and (iii) an independent review.[6] 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. In all cases, however, a bank's operational risk

---

[5] Operational risk is defined 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.

[6] As discussed in the Committee's paper *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches*, June 2011, independent review includes the following components:

Verification of the Framework 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 parties from external sources. Verification activities test the effectiveness of the overall Framework, 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 is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk measurement methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of internal validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process.

governance function should be fully integrated into the bank's overall risk management governance structure.

14. In the industry practice, the first line of defence is business line management. This means that sound operational risk governance will recognise that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

15. A functionally independent corporate operational risk function (CORF)[7] is typically the second line of defence, generally complementing the business line's operational risk management activities. The degree of independence of the CORF will differ among banks. For small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

16. The third line of defence is an independent review and challenge of the bank's operational risk management controls, processes and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

17. If operational risk governance utilises the three lines of defence model, the structure and activities of the three lines often varies, depending on the bank's portfolio of products, activities, processes and systems; the bank's size; and its risk management approach. A strong risk culture and good communication among the three lines of defence are important characteristics of good operational risk governance.

18. Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively.[8] Where audit activities are outsourced, senior management should consider the effectiveness of the underlying arrangements and the suitability of relying on an outsourced audit function as the third line of defence.

19. Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the Framework meets organisational needs and supervisory expectations. For example, while internal audit

---

[7] In many jurisdictions, the independent corporate operational risk function is known as the corporate operational risk management function.

[8] The Committee's paper, *Internal Audit in Banks and the Supervisor's Relationship with Auditors,* August 2001, describes the role of internal and external audit.

should not be setting specific risk appetite or tolerance, it should review the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances.

20. Because operational risk management is evolving and the business environment is constantly changing, management should ensure that the Framework's policies, processes and systems remain sufficiently robust. Improvements in operational risk management will depend on the degree to which operational risk managers' concerns are considered and the willingness of senior management to act promptly and appropriately on their warnings.

Fundamental principles of operational risk management

Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management[9] should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture[10] exists throughout the whole organisation.

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Governance[11]

The Board of Directors

Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

Principle 4: The board of directors should approve and review a risk appetite and tolerance statement[12] for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

---

[9] 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 as regards 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.

[10] Internal operational risk culture is taken to mean the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management.

[11] See also the Committee's *Principles for enhancing corporate governance*, October 2010.

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 risk appetite and tolerance.

Risk Management Environment

Identification and Assessment

Principle 6: Senior management should ensure the 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.

Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

Monitoring and Reporting

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

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.

Business Resiliency and Continuity

Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Role of Disclosure

Principle 11: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

---

[12] "Risk appetite" is a high level determination of how much risk a firm is willing to accept taking into account the risk/return attributes; it is often taken as a forward looking view of risk acceptance. "Risk tolerance" is a more specific determination of the level of variation a bank is willing to accept around business objectives that is often considered to be the amount of risk a bank is prepared to accept. In this document the terms are used synonymously.

Fundamental principles of operational risk management

Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

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

22. The board should establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities for risk, as well as their authority to act. Strong and consistent senior management support for risk management and ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, and training programmes. Compensation policies should be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They should also appropriately balance risk and reward.[13]

23. Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organisation. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

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

25. A vital means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organisation

[13] See also: the Committee's *Report on the range of methodologies for the risk and performance alignment of remuneration,* May 2011*;* the Financial Stability Forum's *Principles for sound compensation practices*, April 2009; and the Financial Stability Board's *FSB principles for sound compensation practices – implementation standards*, September 2009.

including those at the group and business line levels, as well as into new business initiatives' products, activities, processes and systems. In addition, results of the bank's operational risk assessment should be incorporated into the overall bank business strategy development processes.

26. The Framework should be comprehensively and appropriately documented in board of directors approved policies and should 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 Framework.

27. Framework documentation should clearly:

(a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities;

(b) describe the risk assessment tools and how they are used;

(c) describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;

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

(e) establish risk reporting and Management Information Systems (MIS);

(f) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives[14];

(g) provide for appropriate independent review and assessment of operational risk; and

(h) require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

Governance

The Board of Directors

Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

28. The board of directors should:

(a) establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank's strategies and activities, and develop comprehensive, dynamic oversight and control

[14] An inconsistent taxonomy of operational risk terms may increase the likelihood of failing to identify and categorise risks, or allocate responsibility for the assessment, monitoring, control and mitigation of risks,

environments that are fully integrated into or coordinated with the overall framework for managing all risks across the enterprise;

(b) provide senior management with clear guidance and direction regarding the principles underlying the Framework and approve the corresponding policies developed by senior management;

(c) regularly review the Framework to ensure that 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);

(d) ensure that the bank's Framework is subject to effective independent review by audit or other appropriately trained parties; and

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

29. Strong internal controls are a critical aspect of operational risk management, and the board of directors should establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business lines and support functions.

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

30. When approving and reviewing the risk appetite and tolerance statement, the board of directors should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent. The board of directors should approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.

31. The board of directors should regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review should consider changes in the external environment, material increases in business or activity 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 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

---

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

organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

32. 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 and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner.

33. Senior management should translate the operational risk management Framework established 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 that the necessary resources are available to manage operational risk in line within 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.

34. 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 outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

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

36. 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.

37. 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 for larger and more complex organisations with a central group function and separate business units is 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 a combination of members with expertise in business activities and financial, as well as independent risk management. Committee membership can also include

independent non-executive board members, which is a requirement in some jurisdictions; and

(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 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.

38. Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors[16] and external factors.[17] Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively.

39. Examples of tools that may be used for identifying and assessing operational risk include:

(a) Audit Findings: While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors.

(b) Internal Loss Data Collection and Analysis: Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic.[18] Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure;

(c) External Data Collection and Analysis: External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organisations other than the bank. External loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures;

---

[16] For example, the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover.

[17] For example, changes in the broader environment and the industry and advances in technology.

[18] Mapping internal loss data, particularly in larger banks, to the Level 1 business lines and loss event types defined in Annexes 8 and 9 of the 2006 Basel II document can facilitate comparison with external loss data.

(d) Risk Assessments: In a risk assessment, often referred to as a Risk Self Assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, Risk Control Self Assessments (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered). Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;

(e) Business Process Mapping: Business process mappings identify the key steps in business processes, activities and organisational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They also can help prioritise subsequent management action;

(f) Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank's risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;

(g) Scenario Analysis: Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process;

(h) Measurement: Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and

(i) Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank determine whether self assessment processes are functioning effectively. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank's exposure to potential risk events.

40. The bank should ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk. Where operational risk is not considered, risk-taking incentives might not be appropriately aligned with the risk appetite and tolerance.

Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

41. In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate 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 bank should ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products activities, processes and systems.

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

(a) inherent risks in the new product, service, or activity;

(b) changes to the bank's operational risk profile and appetite and tolerance, including 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; and

(f) the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

The approval process should also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The implementation of new products, activities, processes and systems should be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.

Monitoring and Reporting

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

43. Banks are encouraged to continuously improve the quality of operational risk reporting. A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Reports should be manageable in scope and volume; 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. 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 Framework performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities should also be reported internally to senior management and the board, where appropriate.

45. Operational risk reports may contain 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:

(a) breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;

(b) details of recent significant internal operational risk events and losses; and

(c) relevant external events and any potential impact on the bank and operational risk capital.

46. Data capture and risk reporting processes should be analysed periodically with a view to continuously 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 five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.[19]

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

(a) top-level reviews of progress towards stated objectives;

(b) verifying 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; and

(e) tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy.

49. An effective control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other countermeasures may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised, and be subject to careful independent monitoring and review.

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

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

(a) clearly established authorities and/or processes for approval;

(b) close monitoring of adherence to assigned risk thresholds or limits;

(c) safeguards for access to, and use of, bank assets and records;

(d) appropriate staffing level and training to maintain expertise;

(e) ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;[20]

(f) regular verification and reconciliation of transactions and accounts; and

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

51. 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.

52. The use of technology related products, activities, processes and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks.[21] Sound technology risk management uses the same precepts as operational risk management and includes:

(a) governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;

(b) policies and procedures that facilitate identification and assessment of risk;

(c) establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk;

(d) implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and

(e) monitoring processes that test for compliance with policy thresholds or limits.

53. Management should ensure the bank has a sound technology infrastructure[22] that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated

---

[20] 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.

[21] Refer also to the Committee's July 1989 paper *Risks in Computer and Telecommunication System*, and its May 2001 paper *Risk Management Principles for Electronic Banking*.

[22] Technology infrastructure 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.

and comprehensive risk management. Mergers and acquisitions resulting in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine a bank's ability to aggregate and analyse information across risk dimensions or the consolidated enterprise, manage and report risk on a business line or legal entity basis, or oversee and manage risk in periods of high growth. Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high growth strategies are initiated, or new products are introduced.

54. Outsourcing[23] is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. 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. Outsourcing policies and risk management activities 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;

(f) development of viable contingency plans; and

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

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.[24]

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

---

[23] Refer also to the Joint Forum's February 2005 paper *Outsourcing in Financial Services*.

[24] See also the Committee's paper, *Recognising the risk-mitigating impact of insurance in operational risk modelling,* October 2010.

mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors 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).

Business Resiliency and Continuity

Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.[25]

57. Banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of their business obligations. Incidents that damage or render inaccessible the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system. To provide resiliency against this risk, a bank should establish business continuity plans commensurate with the nature, size and complexity of their operations. Such plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable.

58. Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes. A bank should identify critical business operations,[26] key internal and external dependencies,[27] and appropriate resilience levels. Plausible disruptive scenarios should be assessed for their financial, operational and reputational impact, and the resulting risk assessment should be the foundation for recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.

59. A bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to management and the board.

---

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

[26] A bank's business operations include the facilities, people and processes for delivering products and services or performing core activities, as well as technology systems and data.

[27] External dependencies include utilities, vendors and third-party service providers.

Role of Disclosure

Principle 11: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

60. 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.

61. A bank should disclose its operational risk management framework in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

62. A bank's disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the bank.[28]

63. A bank should have a formal disclosure policy approved by the board of directors that addresses 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, including the verification and frequency of them.[29]

---

[28] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, Section V (Operational Risk), paragraph 646, Basel, June 2006, paragraph 810.

[29] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, Section V (Operational Risk), paragraph 646, Basel, June 2006, paragraph 821.

Appendix

Reference material

A Framework for Internal Control Systems in Banking Organisations (BCBS, September 1998)

Internal audit in banks and the supervisor's relationship with auditors (BCBS, August 2001)

The relationship between banking supervisors and bank's external auditors (BCBS, January 2002)

Core Principles for Effective Banking Supervision (BCBS, October 2006)

Core Principles Methodology (BCBS, October 2006)

High-Level Principles for Business Continuity (BCBS, August 2006)

Outsourcing in financial services (Joint Forum, February 2005)

Risk Management Principles for Electronic Banking (BCBS, May 2001)

Risks in Computer and Telecommunication Systems (BCBS, July 1989)

Principles for Enhancing Corporate Governance (BCBS, October 2010)

Recognising the risk-mitigating impact of insurance in operational risk modelling (BCBS, October 2010)

High-level principles for the cross-border implementation of the New Accord (BCBS, August 2003)

Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA) (BCBS, November 2007)