Operational Risk Management

Introduction

1. Operational risk is inherent in all banking products, activities, processes and systems. The effective management of operational risk has always been a fundamental element of a banking corporation's risk management program. Accordingly, sound operational risk management is a reflection of the effectiveness of the board of directors and senior management in administering its portfolios of products, activities, processes, and systems. This Directive establishes the requisite rules for the sound management of operational risk in a banking corporation.

2. Risk management encompasses the process of identifying and assessing risks to the a banking corporation, measuring exposures to these risks as the case may be, ensuring that an effective capital planning and monitoring program 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 of directors on the bank's risk exposures and capital positions. Internal controls are typically embedded in a banking corporation's day-to-day business and are designed to ensure, to the extent possible, that corporation activities are efficient and effective, information is reliable, timely, and complete, and the corporation is compliant with applicable laws and regulation.

3. Fundamental principles of operational risk management

(a) The board of directors shall establish a strong risk management culture. The board and senior management shall establish an organizational culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behavior. In this context, the board of directors shall ensure that a strong operational risk management culture exists throughout the banking corporation.

(b) Banking corporations shall develop, implement, and maintain an operational risk management framework that is fully integrated into their overall risk management processes. The framework will depend on a range of factors, including the nature, size, complexity, and risk profile of the banking corporation.

(c) The board of directors shall establish, approve, and periodically review the framework. The board shall oversee senior management to ensure that the policies, processes, and systems are implemented effectively at all decision-making levels.

(d) The board of directors shall approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the banking corporation is willing to assume.

(e) Senior management shall 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 banking corporation, policies, processes, and systems for the management of operational risk in all the banking corporation's material products, activities, processes, and systems consistent with the risk appetite and tolerance.

(f) Senior management shall ensure the identification and assessment of the operational risk inherent in all material products, activities, processes, and systems.

(g) Senior management shall ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

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

(i) Banking corporations shall have a strong control environment that utilizes policies, processes, and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

(j) Banking corporations shall 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.

Application

4. This Directive shall apply to all banking corporations and credit card companies.

Definitions

5. **"Operational risk"** The risk of a loss occasioned by the inadequacy or failure of internal processes, personnel, and systems, or by external events. This definition includes legal risk[1] but does not include strategic risk and reputational risk.

Risk appetite Determination at the overall level of the risk that the banking corporation is willing to assume in consideration of risk/return indicators; generally perceived as a forward-looking view of the acceptance of risk.

Risk tolerance A more specific determination of the amount of variation that the banking corporation is willing to accept above and below its business goals; generally considered the totality of risk that the banking corporation is willing to assume.

In this Directive, these two terms shall be treated as synonymous.

[1] Legal risk includes, but is not limited to, exposure to fines/penalties for punitive damages as a result of supervisory activity as well as private settlements.

Organizational culture

6. The actions of the board of directors and senior management in establishing and applying policies, processes, and systems provide the infrastructure for an appropriate risk management culture.

7. The board shall establish a code of ethics as set forth in Section 15 of Proper Conduct of Banking Business Directive 301 (Board of Directors). The code shall set clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts of interest. Clear expectations and accountabilities shall ensure that banking corporation staff understand their roles and responsibilities for risk, as well as their authority to act.

8. Senior management shall ensure that an appropriate level of operational risk training is available at appropriate levels of the banking corporation. The training provided shall reflect the seniority, role, and responsibilities of the staff members for whom it is intended.

Three lines of defense

9. Appropriate corporate governance of operational risk rests on three lines of defense. The implementation of these three lines varies among banking corporations depending on the nature, size, and complexity of each banking corporation and the risk profile of its activities. In all cases, however, a banking corporation's operational risk governance function should be fully integrated into its overall risk management governance structure.
    - **First line of defense—business line management.** This means that sound operational risk governance shall recognize 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. Support functions such as IT management are part of this first line of defense.
    - **Second line of defense—a functionally independent corporate operational risk function (CORF).** This function complements the business line's

operational risk management activities. The reporting structure of the CORF shall be independent of the business lines that incur risk and shall be responsible for the design, maintenance, and ongoing development of the banking corporation's operational this framework. Other compliance, monitoring, and control functions, such as a compliance and AML officer, a chief accountant, and control of financial reporting, also belong to the second line of defense. The banking corporation shall specify the interfaces among all functions that comprise the second line of defense to assure coordination and cooperation.

- **The third line of defense—internal audit**—helps the board and management to carry out their responsibilities efficiently and effectively. The duties of the internal audit function are spelled out in Proper Conduct of Banking Business Directive 307, "The Internal Audit Function."

Operational risk management framework

10. Since operational risk management is inherent in all products, activities, processes, and business systems, the board of directors and senior management must understand the nature and complexity of the risks intrinsic to the banking corporation's portfolio of products, services, and activities.

11. The elements of the operational risk framework shall be fully integrated into the overall risk management processes at all levels of the banking corporation, including group and business lines, as well as in new business initiatives, products, activities, systems, and processes. In addition, the results of the banking corporation's operational risk assessment shall be assimilated into the processes used to develop the banking corporation's overall business strategy.

12. The framework shall be comprehensively and appropriately documented in board of directors approved policies and should include definitions of operational risk and operational loss.

13. The framework documentation shall 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 banking corporation'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 banking corporation'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;

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

(h) require review and, where appropriate, revision of the policies whenever a material change in the operational risk profile of the banking corporation occurs.

Corporate governance

a. Board of directors

14. The board of directors is responsible for:

(a) establishing a management culture and supporting processes to understand the nature and scope of the operational risk inherent in the banking corporation's strategies and activities, and developing comprehensive, dynamic oversight and control environments that are fully integrated into or coordinated with the overall framework for managing all risks at the banking corporation;

(b) providing senior management with clear guidance and direction regarding the principles underlying the framework and approving the policy developed by senior management;

(c) regularly reviewing the framework to ensure that the banking corporation has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as operational risks associated with new products, activities, processes, or systems, including changes in risk profiles and priorities (e.g., changing business volumes);

(d) ensuring that the banking corporation's framework is subject to effective independent review by the internal audit function; and

(e) ensuring that management is availing itself of best practices as have evolved in the banking industry.

15. The board of directors shall establish clear lines of management responsibility and accountability for the assimilation of a strong control environment. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business lines, and support functions.

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

17. The board of directors shall review, at least annually, the appropriateness of the limits and the overall operational risk appetite and tolerance statement. This

review shall 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 shall monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

b. Senior management

18. Senior management shall 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 shall clearly assign authority, responsibility, and reporting relationships to encourage and maintain accountability and shall ensure that the necessary resources are available to manage operational risk in line within the risk appetite and tolerance statement. Senior management shall also ensure that the management oversight process is appropriate for the risks inherent in a given business unit's activity.

19. Senior management shall 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 at the banking corporation who are responsible for the procurement of external services such as insurance and outsourcing arrangements.

20. Senior management shall ensure that banking corporation's activities are carried out by staff that has the necessary experience, technical capabilities, and access to resources. Staff members who are responsible for monitoring and enforcing compliance with the banking corporation's operational risk policy shall have authority independent from the units they oversee.

21. Management shall appoint an operational risk management committee that shall report to the risk management committee of the board of directors. Depending on the nature, size, and complexity of the banking corporation, operational risk committees shall be established on the basis of countries, areas of activity, or functional purviews.

    Composition of the committee—the operational risk committees shall include members who have experience in business and financial activities as well as independent risk management.

    Committee meetings shall be held at appropriate frequencies and shall be given 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.

22. The operational risk management committee shall conduct an annual discussion of risks related to internal and external fraud. The discussion shall address the following points *inter alia*:

    (a) the scope of recent internal and external fraud events (since the date of the previous discussion), including lessons learned;

    (b) statistical analysis of events in recent years (distributed by types of events, severity, the units responsible, trends, etc.) and their implications;

    (c) current risks derived from business changes, structural changes, technological changes, etc.;

    (d) interdepartmental operational implications of certain risks;

    (e) periodic review of control mechanisms to ensure their adequacy commensurate with the changes specified above.

Corporate operational risk management function (CORF)

23. The CORF shall include measurement of operational risk and reporting processes, risk committees, and responsibility for board reporting. An important duty of this

function is to challenge the business lines' inputs to, and outputs from, the banking corporation's risk management, risk measurement, and reporting systems. The CORF should have enough personnel skilled in the management of operational risk to effectively address its many responsibilities.

24. The CORF shall help management to discharge its responsibility for understanding and managing the operational risk, developing and consistently implementing operational risk management policies and processes throughout the banking corporation. Its responsibilities shall include:

    (a) development and assimilation of methodological tools for operational risk assessment and risk reporting systems;

    (b) coordination of operational risk management activities throughout the banking corporation;

    (c) providing business units with training activities and consulting services in operational risk management;

    (d) coordination and liaison with the internal audit function.

25. The managers of the CORF should be parallel in stature to those of other risk management functions such as credit, market and liquidity risk.

Risk Management Environment

a. Identification and assessment

26. Effective risk identification considers both internal factors and external factors, such as:

    (a) the banking corporation's management structure, risk culture, quality of human resource management, organizational changes, and staff turnover;

    (b) the nature of the banking corporation's customers, products, and activities, including sources of business and complexity and scope of transactions;

(c) changes in the external operational environment and trends in the banking industry including political, legal, technological, and economic factors; the competitive environment; and market structure.

27. A banking corporation shall perform an operational risk survey at least once every three years or during a period of up to three years. The survey shall include identification of the risks endemic to various processes, assessment of the risks, and recommendations for their minimization and prioritization.

28. In identifying and assessing operational risk, a banking corporation shall:

(a) **collect and analyze loss data[2]:** Internal operational loss data provide meaningful information for the assessment of a banking corporation's exposure to operational risk and the effectiveness of its 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. To facilitate comparison with external loss data, banking corporations may find it useful to map the internal loss data by Level 1 business lines, as specified in Appendix A of Proper Conduct of Banking Business Directive 206 ("Capital Measurement and Adequacy—Operational Risk"), and to produce a detailed classification of loss events as specified in Appendix B of this Directive. Banking corporations 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.

(b) In addition, banking corporations shall use all or some of the following tools, as the case may be:

(1) **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.

[2] Appendix A specifies eight possible outcomes of an operational loss event. Banking corporations shall include Elements 1–4 in the gathering of internal data and may include Elements 5–8 at their discretion.

(2) **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 organizations other than the banking corporation. 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;

(3) **Risk Self-Assessment (RSA):** in which a banking corporation 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), 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).

This process includes the use of one or more of the following tools:

a. workshops in which various business units assess their risk exposures;
b. checklists on which managers are asked to fill in questionnaires that identify the levels of risk and the related controls;
c. scorecards that weight the residual risks so that the RCSA output may be translated into metrics that yield a relative ranking of the control environment.

(4) **Business process mapping:** in which a banking corporation identifies the key steps in business processes, activities, and organizational functions, as well as 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 prioritize subsequent management action.

(5) **Risk and performance indicators:** risk metrics and/or statistics that provide insight into a banking corporation's risk exposure. Risk indicators

that monitor the main drivers of exposure associated with key risks, known as Key Performance Indicators (KPIs), provide insights into the status of operational processes and may in turn illuminate operational weaknesses, failures, and potential losses. Risk and performance indicators are often paired with escalation triggers that to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;

(6) **Scenario analysis:** a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome.

(7) **Measurement:** Banking corporations may find it useful to quantify their exposure to operational risk by using the outputs of the risk assessment tools as inputs for a model that estimates operational risk exposure. The results of the model may be used in an economic capital process and may be allocated to business lines to link risk and return; and

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

29. Banking corporations shall ensure that operational risk is duly taken into account in their internal pricing and performance measurement systems.

New products and activities

30. A banking corporation's operational risk exposure increases when it engages in new activities or develops new products; enters unfamiliar markets; implements

new business processes or technology systems; assimilates new businesses processes or new technological systems; and/or operates in areas are geographically distant from the head office. Accordingly, a banking corporation shall 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.

31. A banking corporation shall have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process shall consider:

    (a) inherent risks in the new product, service, or activity;
    (b) changes to the banking corporation's operational risk profile and appetite and tolerance, including the risk of existing products or activities;
    (c) necessary controls, risk management processes, and risk mitigation strategies;
    (d) the residual risk;
    (e) changes to relevant risk thresholds or limits; and
    (f) procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

    The approval process shall ensure that an appropriate investment in human resources and technology infrastructure is made before new products are introduced. The assimilation of new products, activities, processes, and systems shall be monitored to identify any material differences to the expected operational risk profile and to manage any unexpected risks.

b. Monitoring and Reporting

32. A banking corporation shall ensure that its reports are comprehensive, accurate, consistent, and actionable across business lines and products.

33. The timing and frequency of reporting shsll reflect the risks involved and the pace and nature of changes in the banking corporation's operating environment.

The regular reports submitted to management and the board of directors shall include the outcomes of the monitoring activities and an evaluation of the framework by the internal audit function. Reports generated by (and/or for) Supervisor of Banks shall also be forwarded to senior management and the board.

34. Operational risk reports shall include:
    (a) breaches of the banking corporation'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 banking corporation and operational risk capital.

35. Data capture and risk reporting processes shall be analyzed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

c. Risk control and mitigation

36. A banking corporation shall comply with the March 1998 Basel guidance, *A Framework for Internal Control Systems in Banking Organizations.* An adequate internal control system is comprised of five elements that are inseparable parts of the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.

37. 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 the banking corporation's 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

38. A banking corporation shall identify areas in which duties present individual staff members or teams with potential conflicts of interest, shall minimize them, and shall subject them to independent monitoring and reviews.

39. A banking corporation shall have in place other internal controls for the treatment of operational risk, including:

(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, banking corporation assets and records;

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

(e) processes to identify business lines or products where returns appear to be out of line with reasonable expectations, e.g., risky trade activity and narrow profit margins that yields high returns;

(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 as set forth in Proper Conduct of Banking Business Directive 360 ("Rotation and Uninterrupted Vacation").

40. In addition to the provisions in Proper Conduct of Banking Business Directive 357 concerning IT management, banking corporations shall take an integrated approach toward the identification, measurement, monitoring, and management of operational risk, including:

(a) governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the banking corporation'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 and mitigation strategies; and

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

41. Management shall ensure that the banking corporation has a sound technology infrastructure (relating to the physical and logical structure of information technology and communication systems, individual hardware and software components, data, and the operational environment) that meets current and long-term business requirements by:

(a) providing sufficient capacity for normal activity levels as well as peaks during periods of market stress;

(b) ensuring data and system integrity, security, and availability; and

(c) supporting integrated and comprehensive risk management.

Management shall 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.

42. Outsourcing is the use of a third party to perform activities on behalf of the banking corporation. Outsourcing can involve transaction processing or business processes. 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. Outsourcing policies and risk management activities shall 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) programs 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 banking corporation and at 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 banking corporation.

(h) mandatory assurance that outsourcing arrangements shall not compromise the banking corporation's ability to meet its obligations to customers and shall neither impair nor impede the work of the Banking Supervision Department.

43. Insofar as 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 shall determine the maximum loss exposure that the banking corporation is willing and has the financial capacity to assume and shall perform an annual review of the banking corporation's risk and insurance management program.

44. Banking corporations shall view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. In this context, careful consideration shall be given to the extent to which risk mitigation tools such as insurance truly mitigate risk, transfer the risk to another business sector or area, or create a new risk (e.g., legal or counterparty risk).

Business Resiliency and Continuity

45. Business continuity management is a significant part of operating risk management. Accordingly, banking corporations shall have in place a framework

that is integrated into their risk management program, as set forth in Proper Conduct of Banking Business Directive 355, "Business Continuity Management."

Appendix A. Possible Elements of an Operational Loss Event that a Banking Corporation Should Include in Internal Data Capture

	Description	Details
Compulsory elements:		
1.	Direct charges to P&L and writedowns	Amounts payable occasioned by an operational loss event and the cost of replacing assets or restoring assets to pre-event condition
2.	External costs incurred as a consequence of the event	Legal expenses directly associated with the event and consultants' fees
3.	Specific provisions taken following the occurrence of a risk event	
4.	Near-mess events	Operational risk events that did not cause a loss
Discretionary elements:		
5.	Pending losses	Losses from an operational risk event that have a clear effect, are quantifiable, and are provisionally recorded in transitional accounts and not yet recognized in P&L
6.	Timing losses	
7.	Operational risk gain events	Operational risk events that create a profit
8.	Opportunity costs/lost revenues	Operational risk events that prevent the occurance of future business activity