National Bank of the Republic of Macedonia
Supervisory Policy Manual

Title: OR-1 Operational Risk

Date: FINAL

Purpose: To set out the approach which the NBRM will adopt in the supervision of licensed institutions' operational risk, and to provide guidance to licensed institutions on the key elements of effective operational risk management.

Issue Type: Supervisory Guidance

Supersedes Previous Issue: None

Application: All licensed institutions and supervision personnel

Content:

1. Introduction

1.1. Background

1.1.1. Operations risk affects the long-term existence of an institution, and arises from breakdowns in corporate governance or internal controls. Such breakdowns can lead to financial losses through error, fraud, or failure to perform in a timely manner or cause the interests of the institution to be compromised in some other way; for example, by its dealers, lending officers or other staff exceeding their authority or conducting business in an unethical or risky manner. Other aspects of operations risk include major failure of information technology systems or events such as major fires or other disasters.

1.1.2. As set out in the NBRM's risk-based supervisory approach, there are seven inherent risks present in all licensed institutions. These risks are credit, market, liquidity, information technology, operational, reputation, legal and strategic. Licensed institutions are expected to establish a sound and effective risk management system to manage each of these risks. This guidance focuses on operational risk.

1.1.3. The exact approach for operational risk management chosen by an individual institution will depend on a range of factors, including its size and sophistication and the nature and complexity of its activities. However, despite these differences, clear strategies and oversight by the Supervisory Board (Board) and Board of Directors (Directors), a strong *operational risk culture* and internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal reporting, and contingency planning are all crucial elements of an effective operational risk management framework for institutions of any size and scope.

1.1.4. Operational risk is a term that has a variety of meanings within the banking industry, and therefore for internal purposes, licensed institutions may choose to adopt their own definitions of operational risk. Whatever the exact definition, a clear understanding by licensed institutions of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important that the definition considers the full range of material operational risks facing the institution and captures the most significant causes of severe operational losses. The NBRM will accept a definition of operational risk defined by the Basel Committee under its revised framework on capital standards for banks ("Basel II") as **"the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"**.

1.1.5. Operational risk event types that the NBRM has identified as having the potential to result in substantial losses include:

- Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.

- External fraud. For example, robbery, forgery, check kiting, and damage from computer hacking.
- Employment practices and workplace safety. For example, workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability.
- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the institution's account, money laundering, and sale of unauthorized products.
- Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.
- Business disruption and system failures. For example, computer hardware and software failures, telecommunication problems, and utility outages.
- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty nonperformance, and vendor disputes.

1.1.6. Operational risk has become an increasing issue over the last few years as institutions:

- Greater use and rely on highly automated technology;
- Develop more complex products;
- Become involved in large scale mergers and acquisitions;
- Initiate consolidation and internal reorganization;
- Adopt techniques which are devised to mitigate other forms of risks (e.g. collateralization, credit derivatives, netting and asset securitization), but potentially create other forms of risk (e.g. legal risk); and
- Outsource some of their functions.

Failure to implement proper processes and procedures to control operational risks has resulted in significant operational losses for some institutions in recent years.

1.1.7. In the past, institutions relied almost exclusively upon internal control mechanisms within business lines, supplemented by the audit function, to manage operational risk. While these remain important, recently there has been an emergence of specific structures and processes aimed at managing operational risk. In this regard, an increasing number of organizations have concluded that an operational risk management program provides for safety and soundness, and are therefore making progress in addressing operational risk as a distinct class of risk similar to their treatment of credit and market risk.

1.1.8. In February 2003, the Basel Committee issued a paper entitled "Sound Practices for the Management and Supervision of Operational Risk" for use by licensed and supervisory authorities when evaluating operational risk management policies and practices. The Basel Committee believes that the principles outlined in the Paper establish sound practices relevant to institutions of any size and scope. Therefore, it recommends compliance with its guidance set out in the Paper for all approaches to measuring an operational risk capital charge under Basel II. It also requires that use of the more advanced measurement approaches, i.e. the Standardized Approach (STO) (and Alternative Standardized Approach (ASA)) or the Advanced Measurement Approaches (AMA) be conditional upon the fulfillment of specific operational risk management criteria.

1.2. Scope

1.2.1. This Guidance:

- Sets out the NBRM supervisory approach to operational risk;
- Provides guidance on the key elements of a sound operational risk management framework; and
- Provides additional guidance on how the qualitative criteria for using the STO (or ASA) to calculate operational risk capital charge under Basel II may be met by licensed institutions.

1.2.2. In developing this module, the NBRM has made reference to:

- The Paper issued by the Basel Committee as mentioned under Section 1.1.8 above;
- The qualifying criteria for adopting the STO (or ASA) to calculate operational risk capital charge under Basel II;
- The operational risk management policies and practices adopted by various international institutions; and
- Principle 13 of the “Core Principles for Effective Banking Supervision” covering banks’ risk management processes for controlling other material risks (including operational risk) (the relevant information is contained in the Basel Committee paper on "Core Principles Methodology" (1999)).

1.2.3. For the purpose of this guidance, there is no standard measure of materiality, criticality or significance of an operational event or exposure as it varies among institutions. In determining the relative significance of an operational event or exposure, Institutions may take into account both qualitative and quantitative factors that are relevant to their own circumstances and assess both the current and future impact of such factors on their capital, earnings, franchise and/or reputation.

2. Supervisory Approach to Operational Risk

2.1. Objectives and Principles

2.1.1. Each institution should develop and maintain an appropriate operational risk management framework that is effective and efficient in identifying, assessing, monitoring and controlling/mitigating operational risk. Each institution will need to consider its complexity, range of products and services, organizational structure, and risk management culture as it develops its operational risk management framework.

2.1.2. The NBRM adopts a risk-based supervisory approach which enables continuous supervision of institutions' operational risk through a combination of on-site examinations, off-site reviews and prudential meetings. The objective is to assess, among other things, the level and trend of the institution's operational risk exposures and losses as well as the adequacy and effectiveness of its operational risk management framework. In the case of a locally incorporated institution, the NBRM will also assess the adequacy of its capital relative to the size of its exposure.

2.1.3. In assessing an institution's exposure to and management of operational risk, the NBRM will have particular regard to the following factors:

- The appropriateness of the institution's operational risk management framework, including the level of oversight exercised by the Board and Directors, and risk culture;
- The adequacy of policies, strategies and procedures for managing operational risk, including the definition of operational risk;
- The adequacy of the operational risk management processes in identifying, assessing, monitoring and controlling operational risks;
- The effectiveness of an institution's operational risk management efforts;
- The findings and recommendations made in the management letter issued by the institution's external auditors;
- The causes and impacts of significant operational risk events;
- The institution's procedures for the timely and effective resolution of operational risk events and vulnerabilities;
- The quality and comprehensiveness of an institution's disaster recovery plan and business continuity plan (BCP).

2.2. Supervisory Processes

2.2.1. The NBRM will require that all institutions, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

2.2.2. The NBRM will conduct, directly or indirectly, regular independent evaluation of an institution's policies, procedures and practices related to operational risks. The NBRM will take appropriate enforcement actions to ensue that there are appropriate mechanisms in place to manage operational risk. Independent evaluations of each licensed institution for operational risk will include determining and/or assessing the following:

- The effectiveness of the risk management process and overall control environment with respect to operational risk;
- The methods for monitoring and reporting its operational risk profile, including overseeing the sensitivity of operational risk and operational losses and other indicators of potential operational risk;

- The procedures for the timely and effective resolution of operational risk events and vulnerabilities;
- The process of internal controls, reviews and audits to ensure the integrity of the overall operational risk management process;
- The effectiveness of operational risk mitigation efforts, such as the use of insurance;
- The quality and comprehensiveness of the disaster recovery and business continuity plans; and
- The process for assessing overall capital adequacy for operational risk in relation to its risk profile and, if appropriate, internal capital targets.

2.2.3. Deficiencies identified during the supervisory review may be addressed through a range of actions. The NBRM will use the tools most suited to the particular circumstances of the institution and its operating environment. In order that supervisors receive current information on operational risk, they may wish to establish reporting mechanisms, directly with institutions and external auditors (for example, internal management reports on operational risk could be made routinely available to supervisors).

2.2.4. Given the general recognition that comprehensive operational risk management processes are still in development at many institutions, the NBRM will take an active role in encouraging ongoing internal development efforts by monitoring and evaluating an institution's recent improvements and plans for prospective developments. These efforts can then be compared with those of other institutions to provide the subject institution 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. In addition, the NBRM will focus on the extent to which an institution has integrated the operational risk management process throughout its organization to ensure effective business line management of operational risk, to provide clear lines of communication and responsibility, and to encourage active self assessment of existing practices and consideration of possible risk mitigation enhancements.

3. Operational Risk Management Framework

3.1. Overview

3.1.1. Sound operational risk management will have to be developed into a functional discipline with dedicated staff using established formal policies and processes. This is driven by a growing recognition by Boards and Directors of the need to address operational risk as a distinct class of risk (such as credit risk or market risk) for increased risk awareness, protection of reputation, reduced losses, and ultimately protection and enhancement of shareholder value. Nevertheless, it is clear that operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process.[1] At the same time, failure to properly manage operational risk can result in a misstatement of an institution’s risk profile and expose the institution to significant losses.

3.1.2. Institutions should identify and assess the operational risk inherent in all material products, activities, processes and systems. Institutions should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

3.1.3. Institutions should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to Directors and the Board that supports the proactive management of operational risk.

3.1.4. Institutions should have policies, processes and procedures to control and/or mitigate material operational risks. Institutions should periodically review their risk limitation and control strategies and adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

3.1.5. Finally, institutions should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

3.2. Appropriate Framework

3.2.1. Regardless of its size or complexity, each institution is expected to develop an appropriate framework for managing operational risk. The objective of an operational risk management framework is to ensure that operational risks are consistently and comprehensively identified, assessed, mitigated/controlled, monitored and reported.

3.2.2. For the purpose of this guidance, an appropriate operational risk management framework is considered to consist of the following components:

- Organizational structure (including Board oversight, Directors responsibilities, roles of business line management, an operational risk management function and internal audit);
- Risk culture;
- Strategy and policy (operational risk management strategy, policies and procedures); and
- Operational risk management process (the processes to identify, assess, monitor, control/mitigate and report operational risk).

[1] The NBRM recognizes that in some business lines with minimal credit or market risk (e.g., asset management, and payment and settlement), the decision to incur operational risk, or compete based on the ability to manage and effectively price this risk, is an integral part of a institution’s risk/reward calculus

3.3. Risk Identification and Assessment

3.3.1. In order to better understand its operational risk profile and effectively target risk management resources, an institution should identify the types of operational risk that it is exposed to as far as reasonably possible and assess its vulnerability to these risks. It should identify and assess the operational risk inherent in all existing or new, material products, activities, processes and systems, based on its own definition and categorization of operational risk. Effective operational risk identification and assessment processes are paramount for the subsequent development of a viable operational risk monitoring and control system.

3.3.2. When identifying its operational risk, an institution should consider both internal and external factors that could adversely affect the achievement of the its objectives, such as:

- The management structure, risk culture, human resource management practices, organizational changes and employee turnover;
- the nature of the customers, products and activities, including sources of business, distribution mechanisms, and the complexity and volumes of transactions;
- The design, implementation, and operation of the processes and systems used in the operating cycle of products and activities; and
- The external operating environment and industry trend, including political, legal, technological and economic factors, the competitive environment and market structure.

3.3.3. Having identified the risks, institutions need to define the appropriate approach to assessing each identified risk, estimate the probability that the identified risks will materialize by considering the causes of the risks, and assess their impact by referring to the potential effect on the realization of corporate objectives.

3.3.4. A number of tools are commonly used for identifying and assessing operational risk:

- *Self or Risk Assessment* – an institution assesses its operations and activities against a menu of potential risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment.
- *Risk Mapping* – in this process, various business units, organizational functions or process flows are mapped by risk types. This exercise can reveal areas of weakness and help prioritize subsequent management action.
- *Risk Indicators* – risk indicators are statistics and/or metrics, often financial, which can provide insight into an institution’s risk position. These indicators tend to be reviewed on a periodic basis (such as quarterly, monthly) to alert management to changes that may be

indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions, etc.

3.3.5. If conducted effectively, self-assessment should result in the identification of control gaps, and consequently the appropriate corrective actions to be taken (or a specific statement to accept the exposure) with a clear indication of the lines of responsibility for implementing the corrective actions and a target completion date. As such, the process should make the risk analysis of an institution explicit, clarify accountability in the line business areas, and ensure oversight by Directors and other senior managers.

3.3.6. In order to understand the effects of its operational risk exposures, an institution should continually assess its operational risks, taking into account factors such as:

- Actual operational loss events or events that could have resulted in significant operational losses but were avoided (e.g., near misses or penalties waived by counterparty as a gesture of goodwill);
- Results of internal assessment of risks and controls;
- Figures or trends shown in risk indicators (i.e. quantitative data which can demonstrate operational efficiency, e.g., settlement failures, staff turnover, system downtime, processing volumes and number of errors, or effectiveness of controls, e.g., audit score or number of audit exceptions, limit excesses);
- Reported external, operational losses and exposures; and
- Changes in its business operating environment.

3.3.7. Methodologies to quantify operational risk are developing. As an institution aims to become more sophisticated in quantifying operational risks, complete and accurate data on operational loss events (by categories of risk) and potential sources of operational loss need to be collected. An established and complete loss event database can potentially be used for empirical analysis and modeling of operational risk as well as quantification of the associated loss. Its importance is being recognized for more effective measurement and management of operational risk.

3.4. Risk Monitoring and Reporting

3.4.1. Institutions should implement a process to monitor their operational risk profiles and material exposures to losses on an on-going basis. The process should include both qualitative and quantitative assessment of exposure to all types of operational risk, assessing the quality and appropriateness of corrective/mitigation actions, and ensuring that adequate controls and systems are in place to identify and address problems before they become major concerns. It should be appropriate to the scale of risks and activities undertaken by the institution.

3.4.2. In monitoring its operational risks, the institution should identify or develop appropriate indicators that provide management with early warning of operational risk issues (often referred to as "key risk indicators" (KRIs)). KRIs used should provide management with predictive information and reflect potential sources of operational risk so that management can act on issues before they become major problems to the institution. KRIs are primarily a selection from a pool of operations/control indicators identified and being tracked by various functions of an institution on a periodic basis, which are considered to be relevant for management tracking and escalation triggering. By setting appropriate "goals or limits" or "escalation triggers" to KRIs, monitoring of the KRIs can provide early warning of an increase in operational risk or a breakdown in operational risk management and facilitate communication of potential problems to a higher level of management.

3.4.3. Risk monitoring should be an integrated part of an institution's activities, the frequency of which should reflect the risks involved in the institution's activities as well as the frequency and nature of changes in the operating environment.

3.4.4. The results of monitoring activities, findings of compliance reviews performed by internal audit and/or the risk management function, management letters issued by external auditors, and reports generated by supervisory authorities, as appropriate, should be included in regular reports to the Board and Directors to support proactive management.

3.4.5. In general, the Board should receive sufficient high-level information to enable them to understand the institution's overall operational risk profile and focus on the material and strategic implications for the business.

3.4.6. Directors should ensure that regular management reports on operational risk are received by the relevant level of management, on a timely basis and in a form and format that will aid in the monitoring and control of their business areas. Risk reports to Directors should be from appropriate areas such as business units, support functions, the operational risk management function and internal audit.

3.4.7. Generally, management reports should contain relevant internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. They should aim to provide information such as:

- Critical operational risks facing, or potentially facing, the institution (e.g., as shown in KRIs and their trend data, changes in risk and control self-assessments, comments in audit/compliance review reports, etc.);
- Major risk events/loss experience, issues identified and intended remedial actions;
- Status and/or effectiveness of actions taken; and
- Exception reporting (covering among others authorized and unauthorized

deviations from the institution's operational risk policy and likely or actual breaches in predefined thresholds for operational exposures and losses).

3.4.8. Reports should be analyzed with a view to improving existing management performance as well as developing new risk management policies, procedures and practices.

3.4.9. To ensure the usefulness and reliability of the reports received, Directors and other senior managers should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general.

3.4.10. Institutions may consider keeping tracked information provided in the reports, particularly the loss data, to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on loss events.

3.5. Risk Control and Mitigation

3.5.1. Institutions should have policies, processes and procedures to control and/or mitigate operational risks. They should also have a system in place for ensuring compliance with a documented set of internal policies concerning the institutions' risk management system. Principle elements of this could include, for example:

- Top level reviews of the institution's progress towards stated objectives;
- Policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
- A system of documented approvals and authorizations to ensure accountability to an appropriate level of management.

3.5.2. Institutions should ensure that the risk management control infrastructure keeps pace with growth or changes in the business activity (e.g., new products, operations in branches/subsidiaries remote from head office, and entry into unfamiliar markets).

3.5.3. A critical element to an institution's control of operational risk is the existence of a sound internal control system. When properly designed and consistently enforced, a sound internal control system will help management safeguard the institution's resources, produce reliable financial reports, and comply with laws and regulations. Sound internal controls will also reduce the possibility of significant human errors and irregularities in internal processes and systems, and will assist in their timely detection when they do occur.

3.5.4. Typical practices to control operational risk in an institution include:

- Segregation of duties to avoid a conflict of interest in the responsibilities of individual staff which can facilitate concealment of losses, errors or inappropriate actions;

- Close monitoring of adherence to assigned risk limits or thresholds and investigation into breaches;
- Maintaining safeguards for access to, and use of, assets and records;
- Ensuring that staff have appropriate expertise and training;
- Identifying business lines or products where returns appear to be out of line with reasonable expectations (e.g., 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); and
- Regular verification and reconciliation of transactions

3.5.5. For all material operational risks that have been identified, management should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled or mitigated, management should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

3.5.6. Institutions can transfer certain levels of their operational risks to third parties through risk mitigation products such as insurance. However, management should not view risk mitigation tools as a replacement for internal operational risk controls. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk (e.g., legal or counterparty risk).

3.5.7. In practice, the institution’s operational risk framework must reflect the scope and complexity of business lines, as well as the corporate organizational structure. Each institution’s operational risk profile is unique and requires a tailored risk management approach appropriate for the scale and materiality of the risks present, and the size of the institution. There is no single framework that would suit every institution; different approaches will be needed for different institutions. In fact, operational risk framework will continue to follow rapid development of banking industry and industry trends.

4. Organizational Structure

4.1. Overview

4.1.1. Operational risk management requires the attention and involvement of a wide variety of organisational components, each of which has different responsibilities. It is essential that each of the organisational components clearly understands its role, authority level and accountabilities under the institution’s organisational and risk management structure. All business and support functions should be an integral part of the overall operational risk management framework. The establishment of an independent centralised risk management function can assist the Board and Directors in meeting their responsibility for understanding and managing operational risk.

Moreover, although certain staff may be charged with specific responsibilities in relation to operational risk, all staff of the institution should play a role in the identification and management of operational risk.

4.2. Supervisory Board Oversight

4.2.1. The Supervisory Board should be aware of the major aspects of the institution's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

4.2.2. The Board should also ensure that the institution's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

4.2.3. Responsibility for operational risk management ultimately rests with the Board. The Board can delegate this responsibility to a designated committee(s) that must:

- Understand the major aspects of the institution's operational risk and a distinct category of risk that should be managed;
- Define the operational risk strategy and ensure that the strategy is aligned with the institution's overall business objectives;
- Approve and periodically review the corporate framework to explicitly manage operational risk, which aims to establish a common definition of operational risk for the institution, principles concerning operational risk management and a common risk management framework, and clear governance and reporting structures for operational risk including roles and responsibilities, standards and tools;
- Review periodic high-level reports on the institution's overall operational risk profile, which identify material risks and strategic implications for the institution;
- Ensure that Directors and other senior managers take necessary steps to implement appropriate policies, processes and procedures within the institution's different lines of business, based on the principles under the Board-approved risk management framework;
- Review the risk management framework regularly to ensure that the institution is managing the operational risks from external market changes and other environmental factors, as well as the operational risks associated with new products, activities or systems;
- Ensure that the operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff; and
- Ensure compliance with regulatory disclosure requirements on operational risk.

4.3. Board of Directors Responsibilities

4.3.1. The Board of Directors should have responsibility for implementing the operational risk management framework approved by the Board. The framework should be consistently implemented throughout the entire organization, and all levels of staff should understand their responsibilities with respect to operational risk management. Directors should also have responsibility for developing policies, processes and procedures for managing operational risk in all material products, activities, processes and systems.

4.3.2. In order to ensure that operational risk policies and procedures are clearly understood and executed, Directors should define the institution's organizational structure for operational risk management and communicate individual roles and responsibilities. It is essential that staff at all levels in the institution clearly understand their individual roles in the operational risk management process.

4.3.3. While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, Directors should clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk effectively. They should also ensure that staff responsible for monitoring and enforcing compliance with the operational risk policy have authority independent from the units they oversee. Moreover, Directors should assess the appropriateness of the operational risk management process in light of the risks inherent in a business unit's activities.

4.3.4. Directors are also responsible for ensuring that sufficient human and technical resources are devoted for operational risk management such that the institution's activities are conducted by qualified staff with the necessary experience and technical capabilities.

4.4. Operational Risk Management Function

4.4.1. It has become a leading practice of institutions to establish a central operational risk management function (at the group and/or corporate level) in a similar manner to institutional credit and market risk functions. The key role of the function is to assist management in meeting their responsibility for understanding and managing operational risk and to ensure the development and consistent application of operational risk policies, processes, and procedures throughout the institution. In so doing it performs a number of roles including:

- Setting corporate-level policies and procedures concerning operational risk management and controls;
- Designing and implementing the institution's operational risk assessment methodology tools and risk reporting systems;

- Coordinating risk management activities across the organization;
- Providing operational risk management training and advising the business units on operational risk management issues, e.g., deployment of operational risk tools; and
- Liaising with internal and external audit.

4.4.2. The operational risk management function will be more effective if its role is performed by an independent risk function in a similar way to that for market and credit risk. In practice, the audit function at some institutions may have initial responsibility for developing an operational risk management program. Where this is the case, institutions should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner. This is to ensure that the independence of internal audit is maintained.

4.4.3. The NBRM recognizes that institutions operate in different ways and are using different operational risk management structures and methodologies. Therefore, it does not propose to prescribe a formal definition of an independent operational risk management function. However, in developing their own organizational structures for operational risk management, institutions should consider how the statures, roles, responsibilities and procedures of different staff functions within the structures can ensure both consistency and completeness in their overall operational risk management.

4.5. Roles of Business Line Management

4.5.1. Business line management is accountable on a day-to- day basis for managing and reporting operational risks specific to their business units. They must ensure that internal controls and practices within their business line are consistent with the institution's firm-wide policies and procedures to support the management of the institution's operational risk. They should ensure that business-specific policies, processes, procedures and staff are in place to manage operational risk for all material products, activities, and processes. Implementation of the operational risk management framework within each business line should reflect the scope of that business line and its inherent operational complexity and operational risk profile. Business line management must be independent of the institution's firm-wide operational risk management function.

4.5.2. To facilitate management of operational risk within each business unit, good practice suggests that there should be dedicated operational risk staff in the business units. These staff members usually have dual reporting lines. While they have a direct reporting relationship in the business unit, they work closely with the central risk management function to assure consistency of policy and tools, as well as to report results and issues. Their responsibilities may include development of risk indicators, determining escalation triggers and providing management reports. To be effective, such staff should be given sufficient empowerment and resources to carry out their responsibilities.

4.6. Other Operational Risk Related Functions

4.6.1. There are a number of other operational risk related staff functions within an institution that should play a role in the operational risk management of an institution. These include specialist departments such as legal and compliance, human resources, information technology, and finance, which should be responsible for some specific aspect of operational risk and related issues, e.g., the human resources function should be a key participant in the management of "people" risk. These other operational risk related functions should on the one hand be responsible for managing the operational risk in their own area, and on the other provide support to other parties within the organizational structure for operational risk management.

4.7. Role of Internal Audit

4.7.1. Internal audit should provide an independent assessment of the operational risk management framework, including the adequacy of the central operational risk management function. Therefore, it should not have direct operational risk management responsibilities. Institutions should have in place adequate audit coverage to verify that operational risk management policies and procedures have been implemented effectively across the organization. The Board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit program is appropriate to risk exposures. Any operational issues identified and reported in the audit process should be addressed by Directors and other senior managers in a timely and effective manner, or raised to the attention of the Board, as appropriate.

5. Risk Culture

5.1. A successful operational risk management framework, and in particular, the effectiveness of the processes in that framework, is dependent on a positive risk culture. An institution's risk culture encompasses the general awareness, attitude and behavior of its employees to risk and the management of risk within the organization. Factors contributing to a positive risk culture include:

- Business objectives and risk appetite, operational risk management framework and the related roles and responsibilities in implementing the framework must be clearly communicated to staff at all levels, and the staff should understand their responsibilities with respect to operational risk management;
- Directors and other senior managers must have an ongoing role throughout the risk management process and send out a consistent message to the whole organization that they are fully supportive of the risk management framework through their actions and words:
- The Board and Directors should communicate a culture emphasizing high standards of ethical behavior at all levels of the institution. This can be demonstrated through the adoption of a code of conduct and by management setting the example of following it;

- Business and risk management activities must be carried out by qualified staff with the necessary experience, technical capabilities and adequate access to resources; and
- An established environment in which staff can speak out and raise operational risk problems openly without fear of negative consequences.

6. Operational Risk Management Strategy, Policies and Procedures

6.1. Strategy

6.1.1. Operational risk management begins with the determination of the overall strategies and objectives of an institution. Once determined, the institution can identify the associated inherent risks in its strategy and objectives, and thereby establish an operational risk management strategy. Responsibility for defining the operational risk management strategy, and for ensuring it is aligned with overall business objectives, should rest with the Board. In doing so, the Board should provide clear guidance on the institution's risk appetite or tolerance, i.e. what risks the institution is prepared to take in pursuit of its business objectives and what risks are unacceptable.

6.2. Policies

6.2.1. An institution should document its policies for managing operational risk, setting out its strategy and objectives for operational risk management for all key underlying businesses and support processes and the processes that it intends to adopt to achieve these objectives. An institution's corporate operational risk policy should be documented and approved by the Board (or its delegated committee) and communicated clearly to staff at all levels.

6.2.2. The institution's corporate policy for managing operational risk should include:

- The definition of operational risk for the institution, including the types of operational risk that are faced by the institution and its customers;
- The risk appetite and tolerance for operational risks;
- The approach to identifying, assessing, monitoring, and controlling its operational risks;
- An outline of the reporting framework and types of data/information to be included in risk management reports; and
- The organizational structure, which defines operational risk management roles, responsibilities and reporting lines of the Board, committees, Directors, the risk management function, business line management and other operational risk related functions.

6.2.3. The corporate policy should be supported by a set of principles that apply to specific components of operational risk, such as new customer approval, new product approval, new systems approval, outsourcing and business continuity planning.

6.2.4. Business line managers are responsible for managing risks in their particular business units. Therefore, they are required to develop supplementary procedures specific to their business, based on and consistence with the corporate operational risk management policy.

6.3. Definition of Operational Risk Components

6.3.1. In order to be able to efficiently identify, assess, monitor and report operational risk within an institution, it is necessary to define the underlying components of operational risk for consistent use across the organization. The definition should consider the full range of material operational risks facing the institution and capture the most significant causes of severe operational losses. A formal and detailed definition is also essential for improving communications, setting accountability, characterizing and accumulating events for modeling and analysis, and consistently sharing experiences and ideas.

6.3.2. The Basel Committee defines operational risk by referring to the four underlying causes of operational risk – process, people, systems and external events (or environment). The definition seeks to delineate operational risks from other risks by referring to key internal and external aspects of an institution's operation that, alone or in combination, can cause operational losses. The following table provides an example of risk cause categories under each of the four underlying causes of operational risk:

Risk Cause Factors	Risk Cause Categories

Process	Inadequate/inappropriate guidelines, policies & procedures;
	Inadequate/failure of communication;
	Erroneous data entry;
	Inadequate reconciliation;
	Poor customer/legal documentation;
	Inadequate security control;
	Breach of regulatory & statutory provisions/requirements;
	Inadequate change management process;
	Inadequate back up/contingency plan; and
	Breach of internal guidelines, policies & procedures.

People	Breach of delegated authority; Criminal acts (internal); Inadequate segregation of duties/dual controls; Inexperienced staff; Staff oversight; and Unclear roles & responsibilities.
System	Inadequate hardware/network /server maintenance; Criminal acts; and Vendor misperformance.
External	Man-made disaster; Natural disaster; and Political/legislative/regulatory causes.

6.3.3. Furthermore, to facilitate measuring operational risks and assessing their potential impact, many institutions have adopted definitions with categories of risk events (i.e. actual loss or loss events) and effects (i.e. the types of financial implications) to supplement the cause categories. (The Basel Committee has developed a matrix with seven broad categories of operational loss event types that are further broken down into sub-categories and related activity examples). Collection and analysis of operational loss data on the basis of these loss event types are required under the AMA of Basel II. In considering and stating their definition of operational risk in their policy, institutions may adopt the Basel matrix as a generic scope. A more detailed definition of operational risk will facilitate assessment, monitoring and reporting of operational risk on a consistent and an aggregate (i.e. group/institution level) basis.

7. Operational Risk Management Process

7.1. Overview

7.1.1. Institutions should identify and assess the operational risk inherent in all material products, activities, processes and systems. Institutions should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

7.1.2. Risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification considers both internal factors (such as the institution’s structure, the nature of its activities, the quality of its human resources, organizational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of objectives. In addition to identifying the most potentially adverse risks, institutions should assess their vulnerability to these risks. Effective risk assessment allows for better understanding of an institution’s risk profile and most effectively target risk management resources.

7.2. Risk Management Tools

7.2.1. Amongst the possible tools used by institutions for identifying and assessing operational risk are:

- *Self- or Risk Assessment*: an institution assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them. In addition, scorecards may be used by institutions to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

- *Risk Mapping*: in this process, various business units, organizational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritize subsequent management action.
- *Risk Indicators*: risk indicators are statistics and/or metrics, often financial, which can provide insight into an institution's risk position. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert management to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.
- *Measurement*: some organizations have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on an institution's historical loss experience could provide meaningful information for assessing the exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events.

7.3. Monitoring

7.3.1. Institutions should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to Directors and the Board that supports the proactive management of operational risk.

7.3.2. An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

7.3.3. In addition to monitoring operational loss events, institutions should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators an effective monitoring process can help identify key material risks in a transparent manner and enable management to act upon these risks appropriately.

7.3.4. The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of an institution's activities. The results of these monitoring activities should be included in regular management and Board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities may also include this type of monitoring and should likewise be reported internally to Directors and the Board, where appropriate.

7.4. Reporting

7.4.1. Directors and other senior managers should receive regular reports from appropriate areas such as business units, group functions, the operational risk management office and internal audit. The operational risk reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and to units of the institution in which areas of concern may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of risk and audit reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports. Reports should be analyzed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

7.4.2. In general, the Board should receive sufficient higher-level information to enable them to understand the institution's overall operational risk profile and focus on the material and strategic implications for the business.

7.5. Policies, Processes and Procedures

7.5.1. Institutions should have policies, processes and procedures to control and/or mitigate material operational risks. Institutions should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile. For all material operational risks that have been identified, management should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, management should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely. Control processes and procedures should be established and institutions should have a system in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principle elements of this could include, for example:

- Top-level reviews of the progress towards the stated objectives;
- Checking for compliance with management controls;

- Policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
- A system of documented approvals and authorizations to ensure accountability to an appropriate level of management.

7.5.2. Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Both the Board and Directors are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of an institution. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

7.5.3. An effective internal control system also requires that there be appropriate segregation of duties and personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and subject to careful independent monitoring and review.

7.5.4. In addition to segregation of duties, institutions should ensure that other internal practices are in place as appropriate to control operational risk. Examples of these include:

- Close monitoring of adherence to assigned risk limits or thresholds;
- Maintaining safeguards for access to, and use of, assets and records;
- Ensuring that staff have appropriate expertise and training;
- Identifying business lines or products where returns appear to be out of line with reasonable expectations (e.g., 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); and
- Regular verification and reconciliation of transactions and accounts.

7.5.5. Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programs can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalize the risk of “low frequency, high severity” losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

7.5.6. However, institutions should view risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly recognize and rectify legitimate 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, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal risk).

7.5.7. Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, institutions should be aware that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the institution's immediate control (e.g., external events). Such problems may cause serious difficulties for institutions and could jeopardize an institution's ability to conduct key business activities. Institutions should establish disaster recovery and business continuity plans that address this risk.

7.5.8. Institutions should also establish policies for managing the risks associated with outsourcing activities. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialized business activities. However, an institution's use of third parties does not diminish the responsibility of the Board and Directors to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing institution. Furthermore, institutions need to manage residual risks associated with outsourcing arrangements, including disruption of services.

7.5.9. Depending on the scale and nature of the activity, institutions should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. The Board and Directors should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the institution for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment. Institutions should carry out an initial due diligence test and monitor the activities of third party providers, especially those lacking experience of the industry's regulated environment, and review this process (including re-evaluations of due diligence) on a regular basis. For critical activities, the institution may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

7.5.10. In some instances, institutions may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organization and should be consistent with the institution’s overall business strategy and appetite for risk.

7.5.11. Institutions should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. For reasons that may be beyond an institution’s control, a severe event may result in the inability of the institution to fulfill some or all of its business obligations, particularly where physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses, as well as broader disruptions to the financial system through channels such as the payments system. This potential requires that institutions establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the institution may be vulnerable, commensurate with the size and complexity of the its operations.

7.5.12. Institutions should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, institutions should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are backed-up at an off-site facility, or where an institution’s operations must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimize the risk that both primary and back-up records and facilities will be unavailable simultaneously.

7.5.13. Institutions should periodically review their disaster recovery and business continuity plans so that they are consistent with current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the institution would be able to execute the plans in the unlikely event of a severe business disruption.