May 2008

Statement of Guidance

Operational Risk Management for Banks

1. STATEMENT OF OBJECTIVES

To provide guidance to banks:

a) on their obligations set out in the Rule on Operational Risk Management for banks, and
b) on the key elements for the implementation of an effective and sound operational risk management framework.

2. INTRODUCTION

2.1. Operational risk is present in virtually all banks' transactions and activities, and has become a significant issue over the last few years, as banks:

a) rely on increasingly complex automated technology;
b) develop more complex products;
c) engage in large-scale acquisitions, mergers, de-mergers and consolidations test the viability of new or newly integrated systems;
d) adopt risk mitigation techniques (e.g., collateral, credit derivatives, netting arrangements and asset securitisation) to optimise their exposure to market risk and credit risk, but which in turn may give rise to other forms of risk (e.g. legal risk); and
e) outsource some of their functions and participate in clearing and settlement systems that can mitigate some risks, but can also present significant other risks.

2.2. The management of specific operational risks is not new, as it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, etc. However, the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk in principle is relatively new. The trends cited in paragraph 2.1 combined with a growing number of high-profile operational loss events worldwide, have led the international banking community to view operational risk management as an inclusive discipline.

2.3. The Statement of Guidance was developed using:

a) the relevant principles outlined in the Basel Committee's "Core Principles for Effective Banking Supervision," relating to operational risk;
b) the Basel Committee's paper entitled "Sound Practices for the Management and Supervision of Operational Risk"; and
c) Operational risk management guidelines adopted by other jurisdictions.

3. SCOPE

3.1. This Statement of Guidance applies to all banks licensed under the Banks and Trust Companies Law (2007 Revision).

4. DEFINITION

4.1. The Basel Committee has defined *Operational Risk* as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." The definition includes legal risk but excludes strategic and reputational risk.

5. GUIDANCE

5.1. Operational Risk Management Framework

5.1.1 Pursuant to Rule 4.1[1], a bank must establish, implement, and maintain an operational risk management framework (strategies, policies, and processes) appropriate for the size, complexity, and nature of its activities. 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.

5.1.2 An operational risk framework should be based on an appropriate definition of operational risk that clearly articulates what constitutes operational risk in the bank. The framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk and the bank's prioritisation of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the bank. It should also include policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk. The degree of formality and sophistication of the bank's operational risk management framework should be commensurate with the bank's risk profile.

5.1.3 At a minimum, an appropriate operational risk management framework should consist of an organisational structure and risk culture (including Board oversight, senior management responsibilities, strategies, policies, processes and internal audit);

[1] Rule on Operational Risk Management for banks

and an operational risk management process (i.e. the processes to identify, assess, monitor, control/mitigate and report operational risk).

5.2. Board Oversight

5.2.1 The Board of directors should be aware of the major aspects of the bank's operational risks as a distinct and controllable risk category that should be managed.

5.2.2 Pursuant to Rule 4.2, the Board of directors is responsible for approving the implementation of an adequate framework[2] for managing operational risk and ensuring that senior management is carrying out its risk management responsibilities. 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.

5.2.3 The Rule also stipulates that the Board reviews the framework regularly to ensure the bank is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems. This review process should also aim to assess industry best practice in operational risk management appropriate for the bank's activities, systems and processes. If necessary, the Board should ensure that the operational risk management framework is revised in light of this analysis, so that material operational risks are captured within the framework.

[2] This will depend on a range of factors such the bank's size and sophistication, and the nature and complexity of activities conducted.

5.2.4 The bank should have in place adequate internal audit[3] coverage to verify that operating policies and procedures are effectively implemented. The Board – either directly, or indirectly through its audit committee – should ensure that the scope and frequency of the audit programme is appropriate to the risks involved. To the extent that the audit function is involved in this process, the Board should ensure that the independence of the audit function is maintained.

5.3. Senior Management responsibilities

5.3.1 Senior management should have responsibility for implementing the operational risk strategy approved by the Board of directors. The strategy should be implemented consistently throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's products, activities, processes and systems.

5.3.2 Senior management should translate the operational risk management strategy established by the Board of directors into policies, processes and procedures that can be implemented and verified. While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management must clearly assign authority, responsibility and reporting

[3] For further guidance on internal audit, please refer to the Authority's SoG on Internal Audit for banks.

relationships to encourage and maintain this accountability. This responsibility includes ensuring that the necessary resources are available to manage operational risk effectively. Moreover, senior management should assess the appropriateness of the management oversight process in light of the risks inherent in a business line's strategy and ensure that staff is apprised of their responsibilities.

5.3.3 Senior management should ensure that sufficient human and technical resources are devoted for operational risk management such that qualified staff with the necessary experience and technical capabilities conduct the bank's activities.

5.3.4 Senior management should ensure that staff responsible for managing operational risk communicates effectively with staff responsible for managing credit, market, and other risks, as well as with those in the firm who are responsible for the procurement of external services such as insurance purchasing and outsourcing agreements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

5.4. Risk Culture

5.4.1 A successful operational risk management framework, and in particular, effectiveness of the processes in that framework, is dependent on a positive risk culture. A bank's risk culture encompasses the general awareness, attitude and behaviour of its employees to risk and the management of risk within the organisation.

5.4.2 The Board and senior management should communicate a culture emphasising high standards of ethical behaviour at all levels of the bank.

5.4.3 Communication flows within the bank should establish a consistent operational risk management culture. Reporting flows should enable senior management to monitor the effectiveness of the risk management system for operational risk, and also enable the Board of directors to oversee senior management performance.

5.4.4 Qualified staff with the necessary experience, technical capabilities, and adequate access to resources should conduct the bank's activities. Also the staff responsible for monitoring and enforcing the institution's risk strategy should have authority independent from the business units they oversee.

5.4.5 The bank's remuneration policies should be consistent with its appetite for risk. Performance incentives should include consideration of risk management and its design should not provide incentives to people to operate contrary to the desired risk management values e.g. established position limits.

5.4.6 Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to such technologies should be well documented and disseminated to all relevant personnel.

5.5. Risk Management: Identification and Assessment

5.5.1 The bank should identify and assess the operational risk inherent in all material products, activities, processes and systems. The bank 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.

5.5.2 Risk identification is critical for the subsequent development of viable operational risk measurement, monitoring and control. Effective risk identification considers both internal factors (such as the complexity of the bank's structure, the nature of the bank's activities, the quality of personnel, organisational changes, employee turnover and the complexity of computer systems and processes) and external factors (such as fluctuating economic conditions, changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives. Other external risks to be considered include natural disaster (hurricane, earthquake, flood), fire, and power outage together with other risks such as acts of terrorism, security breaches, database corruption, viral attacks and system configuration failure.

5.5.3 The risk identification process should be comprehensive and consider all potential risks. There are several processes commonly used by banks to help them identify operational risk:

a) Self- or Risk-Assessment: a bank assesses its operations and activities against a menu of operational risk events. This

process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment

b) Risk Mapping: in this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.

c) Key Risk Indicators: risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators should be reviewed on a periodic basis (often monthly or quarterly) to alert the bank to changes that may be indicative of risk concerns. Such indicators may include for example the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

d) Threshold/limits: typically tied to risk indicators, threshold levels (or changes) in key risk indicators, when exceeded, alert management to areas of potential problems.

e) Measurement: some firms have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk.

5.6. Risk Management Monitoring and Reporting

5.6.1 The bank should establish the processes necessary to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the Board of directors that supports the proactive management of operational risk.

5.6.2 In addition to monitoring operational loss events, the bank 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 could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, and system downtime.

5.6.3 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 the bank's activities. The results of these monitoring activities should be included in management and Board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) the Monetary Authority[4] may also inform this monitoring and should likewise be reported internally to senior management and the Board, where appropriate.

[4] Reports may include on-site inspection reports issued by the Monetary Authority.

5.6.4 Senior management 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 areas of the bank on 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.

5.6.5 The Board of directors should receive sufficient higher-level information to enable them to understand the bank's overall operational risk profile and focus on the material and strategic implications for the business.

5.7. Risk Management: Control and/or Mitigation

5.7.1 The bank should have policies, processes, and procedures to control and/or mitigate operational risks.

5.7.2 The bank should ensure that a system is 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:

a) top level reviews of the bank's progress towards the stated objectives;
b) checking for compliance with management controls;
c) policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and

d) a system of documented approvals and authorizations to ensure accountability to an appropriate level of management.

5.7.3 Control activities should be an integral part of the regular activities of a bank, and should involve all levels of personnel in the bank, including both senior management and business unit personnel. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

5.7.4 The bank 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).

5.7.5 A critical element of a bank's control of operational risk is the existence of a sound internal control system[5]. 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.

[5] For further guidance on internal controls, please refer to the Authority's Rule on Internal Control for all Licensees and SoG on Internal Controls for Banks.

5.7.6 Typical practices to control operational risk in a bank include:

a) 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;
b) close monitoring of adherence to assigned risk limits or thresholds;
c) maintaining safeguards for access to, and use of, bank assets and records;
d) ensuring that staff have appropriate expertise and training;
e) 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
f) regular verification and reconciliation of transactions and accounts.

5.7.7 For all material operational risks that have been identified, the bank 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, the bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

5.7.8 Risk mitigation tools or programmes can be used to reduce the exposure to, frequency and/or severity of certain events (e.g. natural disasters). The bank should view risk mitigation tools as complementary to, rather than a replacement for, thorough

internal operational risk control. Having mechanisms in place to quickly recognise and rectify legitimate operational risk errors can greatly reduce exposures. The bank should also carefully consider 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).

5.7.9 The bank should invest in appropriate processing technology and information technology security commensurate with the size and complexity of operations. However, the bank 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 bank's immediate control (e.g., external events). Such problems may cause serious difficulties for a bank and could jeopardise an institution's ability to conduct key business activities. The bank should therefore establish disaster recovery and business continuity plans that address this risk, as discussed further in Section 5.8.

5.8. Contingency and Business Continuity Plans

5.8.1 The bank should have in place contingency and business continuity plans[6] to ensure its ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

[6] For further guidance on contingency and business continuity plans, please refer to the Authority's SoG on Business Continuity Management for all licensees.

5.9. Outsourcing

5.9.1 The bank should establish sound policies for managing the risks associated with outsourcing activities. Outsourcing of activities has the potential to enhance the bank's performance and can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. However, a bank's use of third parties does not diminish the responsibility of the Board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws.

5.9.2 Outsourcing activities should be based on rigorous robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing bank. Furthermore, the bank should manage and control any residual risks associated with outsourcing arrangements, including disruption of services.

5.9.3 Depending on the nature and scale of the activity, the bank should understand the potential impact on their operations and on their customers of any potential deficiencies in services provided by vendors and other third-party service providers, including both operational breakdowns and the potential business failure or default of the external parties.

5.9.4 The board and management 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 bank for errors, negligence and other operational failures should be explicitly considered as part of the risk assessment. The bank should carry out due diligence tests and monitor the activities of third party providers, especially those lacking experience of the banking industry's regulated environment. For critical activities, the bank 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.