SUPERVISORY AND REGULATORY GUIDELINES: PU-0412
Operational Risk
25th November , 2013

GUIDELINES FOR THE MANAGEMENT OF OPERATIONAL RISK

1. INTRODUCTION

1.1. The Central Bank of The Bahamas ("the Central Bank") is responsible for the licensing, regulation and supervision of banks and trust companies operating in and from within The Bahamas pursuant to the Central Bank of The Bahamas Act, 2000 ("the CBA") and the Banks and Trust Companies Regulation Act, 2000 ("the BTCRA"). Additionally, The Central Bank has the duty, in collaboration with financial institutions, to promote and maintain high standards of conduct and management in the provision of banking and trust services.

1.2. All licensees are expected to adhere to the Central Bank's licensing and prudential requirements and ongoing supervisory programmes and required regulatory reporting, and are subject to periodic on-site examinations. Licensees are also expected to conduct their affairs in conformity with all other Bahamian legal requirements.

2. PURPOSE

2.1. These Guidelines provide guidance to licensees in relation to operational risk management. Licensees are expected to develop and implement an operational risk management framework in line with these Guidelines, taking into account the nature, size, complexity and risk profile of its activities. Licensees are expected to continuously improve their approaches to operational risk management as operational risk continues to evolve.

2.2. These Guidelines are based on the *Principles for the Sound Management of Operational Risk* issued by the Basel Committee on Banking Supervision in 2011 and should be read in conjunction with the following guidelines:

a) *Guidelines for the Corporate Governance of Banks and Trust Companies Licensed to do Business within and from within The Bahamas;*

b) *Business Continuity Guidelines; and*

c) *Guidelines on Minimum Standards for the Outsourcing of Material Functions.*

3. APPLICABILITY

3.1. These Guidelines apply to all licensees, with the exception of nominee trust companies or restricted trust companies whose operations are limited to conducting business on behalf of one client or clients who are members of the same family. The Central Bank recognises that the degree of sophistication of a licensee's operational risk management framework will depend on the nature, size, complexity and risk profile of its activities, as well as the level of operational risk assumed. The Central Bank equally accepts that in the supervision of local subsidiaries of international groups and branches of foreign banks, account should also be taken of the group's operational risk management framework.

4. DEFINITION

4.1. *Operational risk* refers to the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk, but excludes other risks like strategic and reputational risk.

5. OVERVIEW

5.1. Operational risk is potentially inherent in all of a licensee's products, activities, processes and systems and the effective management of operational risk has always been a fundamental element of a bank's risk management program.

5.2. Sound internal governance forms the foundation of an effective operational risk management framework. Operational risk management can vary from one licensee to the next. However, common industry practice for sound operational risk governance often relies on three lines of defence: business line, independent corporate operational risk; and an independent review. The nature, size, complexity and risk profile of a licensee's activities will determine how these three lines of defence are implemented.

5.3. A licensee's governance function should be fully integrated into its overall risk management governance structure. A strong risk culture and good communication among the three lines of defence are important characteristics of good operational risk governance.

Business Line Management

5.3.1. Business line management, as the first line of defence, is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

Independent Corporate Operational Risk Function

5.3.2. The degree of independence of the second line of defence, the corporate operational risk function, will differ among licensees. For small licensees, independence may be achieved through separation of duties and independent review of processes and functions. In larger licensees, the corporate operational risk function will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the licensee. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the corporate operational risk function is to challenge the business lines' inputs to, and outputs from, the licensee's risk management, risk measurement and reporting systems. The function should have a sufficient number of staff skilled in the management of operational risk to effectively address its many responsibilities. The managers of the corporate operational risk function should be of sufficient stature within the licensee to perform their duties effectively.

Independent Review (Internal Audit)

5.3.3. The third line of defence is an independent review and challenge of a licensee's operational risk management controls, processes and systems. Individuals performing the reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the framework.

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

5.3.5. Internal audit coverage should include opining on the overall appropriateness and adequacy of the framework and the associated governance processes across the licensee. Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the framework meets the licensee's needs and supervisory expectations.

5.4. Given that operational risk management is evolving and licensees' business environments are constantly changing, senior management should ensure that the framework's policies, processes and systems remain sufficiently robust.

6. FUNDAMENTAL PRINCIPLES OF OPERATIONAL RISK MANAGEMENT

6.1. The operational risk management strategy chosen by an individual licensee 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 board of directors (the Board) and senior management, 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.

6.2. The Board should take the lead in establishing a strong risk management culture. The Board and senior management should establish a corporate culture, throughout the whole organisation, that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour.

6.3. The Board should establish a code of conduct or ethics policy that sets out clear expectations for integrity and ethical values and ensure that the licensee's employees understand their roles and responsibilities.

6.4. Training on operational risk should be available to all levels throughout the organisation and should appropriately reflect employees' roles and responsibilities.

Components of an Effective Operational Risk Management Framework

6.5. Unlike credit and interest rate risks, operational risk is not undertaken with the expectation of a higher return. Because it occurs naturally in the course of corporate activity, and cannot be readily measured to the same extent as market or credit risks, it is often easily overlooked and poorly managed. To ensure effective operational risk management, the Central Bank requires that the senior management of each of its licensees, under the approval of the board of directors, develop and implement an operational risk management framework (the framework) that explicitly recognizes operational risk as a distinct risk to the institution and aims to efficiently manage it.

6.6. Licensees should develop, implement and maintain a framework that is fully integrated into its overall risk management processes. The framework for operational risk management chosen by an individual licensee will depend on a range of factors, including its nature, size, complexity and risk profile. The framework should be based on a firm-wide definition of operational risk. The scope of the operational risk definition should cover the full range of material

operational risk facing the institution and the most significant causes of operational losses. From this definition, methods of how operational risk is to be identified, assessed, monitored and controlled should be devised

6.7. The Board and senior management should ensure that it understands the nature and complexity of the risks inherent in its products, services and activities/business. A vital means of understanding the nature and complexity of operational risk is to have the components of the framework fully integrated into the overall risk management processes across all levels of the organisation including those at the group and business levels, as well as into new business initiative's products, activities, processes and systems.

6.8. The framework of a licensee should:

a) be comprehensively and appropriately documented in the policies approved by the Board and should include definitions of operational risk and operational loss;

b) identify the organisation structure used to manage operational risk, setting out reporting lines and individuals responsibilities and accountabilities;

c) define the licensee's risk assessment tools and indicate how they are used;

d) define the institution's appetite and tolerance limits for operational risk in its activities and detail the approved risk mitigation strategies and instruments;

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

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

g) define operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;

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

i) require that policies be reviewed whenever a material change in the operational risk profile of the bank occurs and revised as appropriate.

7. GOVERNANCE

Role of the Board of Directors

7.1. The board of directors, in particular, should be aware of the major aspects of the institution's operational risks as they are ultimately responsible and accountable

for managing and controlling operational risks. This section should be read in conjunction with the *Guidelines for the Corporate Governance of Banks and Trust Companies Licensed to do Business within and from within the Bahamas*.

7.2. The Board should:

a) establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank's strategies and activities. Within the institutional structure, the board of directors along with senior management should oversee all risk management functions.

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

c) approve the basic structure of the framework and must periodically review the institution's framework to guarantee that operational risks are being effectively managed;

d) ensure that the framework is subject to effective independent review by internal audit or other appropriately trained parties; and

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

7.3. The board of directors has responsibility for establishing clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business lines and support functions.

7.4. The Board should approve, and review on a regular basis, the risk appetite and tolerance statement that articulates the nature, types and levels of operational risk that the licensee is willing to assume. When approving and reviewing the risk appetite and tolerance statement, the Board should consider all relevant risks, the licensee's risk aversion, its current financial condition and its strategic direction. The Board should also approve the appropriate thresholds/limits for specific operational risks and an overall opearational risk appetite and tolerance. This review should consider changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience and the frequency, volume, or nature of limit breaches. The Board should monitor management adherence to the risk appetite and tolerance statement and provide timely detection and remediation of breaches.

Role of Senior Management

7.5. Following the board of directors' approval of the framework, senior management has responsibility for developing a clear and effective governance structure with well-defined, transparent and consistent lines of responsibility. The governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, licensees should take the following into consideration:

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

7.5.2. It is sound industry practice for operational risk committees (or the risk committee in smaller institutions) to include a combination of members with expertise in business activities, finance and risk management.

7.5.3. Risk committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

7.6. Senior management is also responsible for implementing and maintaining the framework throughout the licensee's business units, its policies, processes and systems for managing operational risk and ensuring they are consistent with the licensee's risk appetite and tolerance. Senior management is also responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes, which include systems to report, track and escalate issues to ensure resolution.

7.7. Senior Management should ensure that, on an ongoing basis, the framework is being implemented consistently throughout the whole institution and that all levels of staff understand their responsibilities with respect to operational risk management. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability and to ensure that the necessary resources are available to manage operational risk in line with the licensee's risk appetite and tolerance statement. Additionally, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit's activities.

7.8. Senior management should also ensure that staff responsible for managing operational risk coordinate and communicate effectively with other staff involved in the business. The licensee's staff should have the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the licensee's risk policy should have authority independent from the units they oversee.

8. RISK MANAGEMENT ENVIRONMENT

Identification and Assessment

8.1. An important feature of any operational risk management framework is its ability to identify and assess the degree of operational risk in an institution's products, activities, processes and systems. Effective risk identification examines internal events such as the institution's structure, the nature of its activities, the quality of its human resources, organizational changes, and employee turnover as well as external events, such as changes in the industry and technological advances in an effort to identify which business components are vulnerable to material operational risks. Sound risk assessment allows institutions to better understand their risk profile and more effectively target risk management resources.

8.2. Examples of some tools that may be used for identifying and assessing operational risk include, but are not limited to:-

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

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

c) External Data Collection and Analysis: External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organisations other than the bank/licensee. 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;

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

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

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

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

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

i) Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the licensee's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank

determine whether self assessment processes are functioning effectively. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank's exposure to potential risk events.

8.3. As the risk profile and appetite of an institution may change over time, the assessment of operational risks should be conducted periodically along with the review of its tolerance levels. The frequency of periodic assessments and reviews is at the discretion of the licensee's Board and senior management. Nonetheless, periodic efforts are necessary as they ensure that material operational risks are captured through the continual update of a licensee's operational risk control strategies, policies, processes, procedures and systems.

8.4. A licensee's operational risk exposure may increase when it engages in new activities or develops new products, enters new or unfamiliar markets, implements new business processes or technology system. The level of risk may also increase when new products activities, processes or systems become a material source of revenue or is a business critical operation. A licensee should ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products activities, processes and systems. Licensees should have policies and procedures that address the process for review and approval of new products, activities, processes and systems, which consider the following:

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

b) changes to the operational risk profile and appetite and tolerance, including the risk of existing products or activities;

c) the necessary controls, risk management processes and risk mitigation strategies;

d) the residual risk;

e) changes to relevant risk thresholds or limits; and

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

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

Monitoring and Reporting

8.6. Licensees should have the appropriate monitoring and reporting mechanisms in place at the Board, senior management and business line levels that support the proactive management of operational risk, but should also be manageable in terms of scope and volume. Licensees are encouraged to continuously improve the quality of operational risk reporting. Reports should be comprehensive, accurate and consistent and actionable across business lines and products. Reports should also be timely and licensees should be able to produce reports in both normal and stressed market conditions. The nature of the risks involved and the frequency of changes in the operating environment should determine the reporting frequency. Reports generated by (and/or for) supervisory authorities should also be reported internally to the Board and senior management, where appropriate.

8.7. Risk monitoring should cover the institution's entire range of operations and all types of material risks inherent in its operations. Particularly, in an effective operational risk management framework, risk indicators and material exposures to losses should be monitored regularly. The results of monitoring activities should be included in the regular reports to the Board and senior management. These reports should highlight items of concern and the areas of the institution that will be impacted and, among other uses, be used to assess the effectiveness of the licensee's risk management and may reveal areas that need improvement.

8.8. Operational risk reports may contain internal financial, operational and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational risk reports should include:

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

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

c) relevant external events and any potential impact on the institution.

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

Risk Control and Mitigation

8.10. Risk control and mitigation is at the heart of operational risk management. Once risks have been identified, assessed and measured, and the institution has decided to bear the risks, these risks must be controlled by having a strong control environment in places that utilises policies, processes and systems, appropriate internal controls and appropriate risk mitigation and/or transfer activities.

8.11. On an ongoing basis, licensees should provide for expected losses and maintain adequate financial resources against unexpected losses that may be encountered in the normal course of their business activities.

A. Internal Controls

8.12. Internal controls should be designed to provide reasonable assurance that a licensee will have efficient and effective operations, safeguard its assets, produce reliable financial reports and comply with applicable laws and regulations. Control processes and procedures should include a system for ensuring compliance with policies. More generally, institutions should ensure that in an effort to control and mitigate operational risks, there are appropriate internal controls. A sound internal control programme consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication and monitoring activities.

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

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

b) verifying compliance with management controls;

c) review of the treatment and resolution of instances of non-compliance;

d) evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management; and

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

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

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

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

b) close monitoring of adherence to assigned risk limits/thresholds or compliance with management controls;

c) safeguards restricting access to, and use of, bank records and assets to authorized personnel;

d) appropriate staffing level and training to maintain expertise;

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

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

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

B. Information Technology Systems

8.16. The effective use and sound implementation of technology may reduce an institution's susceptibility to some human errors, but will increase its dependency on the reliability of information technology systems. It is necessary to be aware that increasing automation of systems and reliance on information technology has the potential to transform minor manual processing errors to major systematic failures.

8.17. Complex or poorly designed IT systems and processes can give rise to operational losses, either because they are not optimally structured, or because they malfunction. Properly functioning systems reduce settlement-processing errors, fraud and information security failures. Hence, licensees should have an integrated approach to identifying, measuring, monitoring and managing technology risks. Sound technology risk management uses the same precepts as operational risk management and includes:

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

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

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

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

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

8.18. Management should ensure that the institution has a sound technology infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress, ensuring data and system integrity, security and availability and supporting in integrated and comprehensive risk management. Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high growth strategies are initiated or new products are introduced.

C. Outsourcing and Insurance

8.19. For the purposes of these Guidelines, outsourcing involves a licensee entering into an arrangement with another party, including an entity affiliated or related to the licensee, to perform a business activity which currently is, or could be, undertaken by the licensee itself. Outsourcing may, in certain circumstances, help manage costs, provide expertise, expand product offerings and improve services. However, if outsourcing arrangements are not managed adequately the degree of operational risk faced by an institution may increase. The Board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and procedures are in place to manage the risk in outsourcing activities. Licensees' outsourcing policies and risk management activities should encompass:

a) procedures for determining whether and how activities can be outsourced;

b) processes for conducting due diligence in the selection of potential service providers;

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

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

e) establishment of an effective control environment at the licensee and the service provider;

f) development of viable contingency plans; and

g) execution of comprehensive service level agreements with a clear allocation of responsibilities between the outsourcing provider and the licensee.

8.20. Licensees are encouraged to review the Central Bank's Guidelines on *Minimum Standards for the Outsourcing of Material Functions (August* 2009). Before entering into, or significantly changing an outsourcing arrangement, an institution should analyse how the proposed outsourcing will affect its overall risk profile and business strategy and its ability to continue to meet the Central Bank's regulatory requirements. To minimize the risks that an outsourcee may pose on an institution, the quality of the outsourcee and the contents of the outsourcing contract must be closely analyzed. In particular, senior management must ensure the proper implementation and maintenance of an outsourcing arrangement so that it retains control of the performance quality of outsourced activities.

8.21. In cases where internal controls do not adequately address risk and exiting the risk is not a reasonable option, the institution may seek to transfer the risk to another party such as through insurance. The Board should determine the maximum loss exposure the institution is willing and has the financial capacity to assume and should perform an annual review of its risk and insurance management programme. Institutions using insurance to cover operational risks should conduct proper due diligence of the insurance carrier and review the insurance policy so as not to incur counterparty risk and, potentially, liquidity risk.

8.22. Risk transfer is an imperfect substitute for sound controls and risk management programmes. Hence, licensees should view risk transfer tools as complementary to, rather than a replacement for, thorough operational risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area or create a new risk. Regardless of the protection that insurance provides, licensees should ensure that the policies and procedures to control operational risks are maintained and that insurance does not decrease the incentive to effectively control/mitigate against operational risks.

Business Resiliency and Continuity

8.23. In accordance with the Central Bank's Business Continuity Guidelines (October 2008), institutions should have 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. Incidents that damage or render inaccessible an institution's facilities, telecommunication or information technology infrastructures, or an event that affects human resources, can result in significant financial losses, as well as broader disruptions to the financial system. Licensees should establish business continuity plans commensurate with the institution's nature, size and the complexity of its operations.

8.24. Business continuity plans should address different types of plausible scenarios in which the licensee's physical, telecommunication, or information technology infrastructures may be damaged or inaccessible. These scenarios should be assessed for their financial, operational and reputational impact and the resulting risk assessment should be the foundation for recovery priorities and objectives.

8.25. Business continuity plans should incorporate business impact analysis, recovery strategies, testing, training and awareness programs and communication and crisis management programmes. Licensees should identify critical business operations, key internal and external dependencies and appropriate resilience levels. Licensees should devise alternate means of resuming their operations should they be severely disrupted. The use of an alternative site for recovery of operations is common practice in business continuity management. Where used, an institution should assess the appropriateness of the alternate site (i.e. the location, speed of recovery, adequacy of resources, etc.). Continuity plans should establish contingency strategies, recovery and resumption procedures and communication plans for informing management, employees, regulatory authorities, customers, suppliers and, where appropriate, other agencies.

8.26. Senior management is responsible for regularly reviewing the plans to make sure they are updated to meet the institution's operational and strategic needs. The plans should also be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, licensees should participate in disaster recovery and business continuity testing with key service providers, the results of which should be reported to the Board and senior management. Training and awareness programmes should also be implemented to ensure that staff can effectively execute contingency plans.

9. DISCLOSURE

9.1. Given that public disclosure improves transparency and strengthens market discipline, the Central Bank encourages licensees to disclose relevant information regarding their operational risk management framework to allow stakeholders to determine whether the licensee identifies, assesses, monitors and controls/mitigates operational risk effectively. Disclosures should be commensurate with the size, risk profile and complexity of a licensee's operations.

10. SUPERVISION OF OPERATIONAL RISK MANAGEMENT

10.1. The Central Bank, as part of its ongoing supervisory responsibilities, intends to assess the degree of licensees' compliance with the principles set forth in these Guidelines, taking into account the nature, size, risk profile and complexity of the

licensee's activities. Consequently, the Central Bank will examine the effectiveness of the operational risk management strategy and framework during the course of its on-site examination of licensees.

END

APPENDIX I

Examples of the events that can give rise to significant operational risks

- Execution, delivery and process management inaccuracies. For example, data entry errors, settlement-processing errors, collateral management failures, incomplete legal documentation

- Internal fraud. For example, intentional misreporting of positions, employee theft, insider trading

- External fraud. For example, robbery, forgery, computer hacking

- Employment practices and workplace safety difficulties. For example, workers compensation claims, organized labour activities, harassment and discrimination claims, other unbudgeted personnel costs

- Damage to physical assets. For example, terrorism, vandalism, hurricanes, floods

- Clients, products and business practice abuses. For example, money laundering, misuse of confidential customer information, sale of unauthorized products, fiduciary breaches, improper trading activities, unapproved access given to client accounts

- Business disruption and system malfunction. For example, hardware and software failures, telecommunication problems, utility outages, information security failures

- Outsourced function/process failures. For example, poor execution of back-office functions, inadequately trained personnel, significant changes in systems and procedures