OPERATIONAL RISK MANAGEMENT GUIDELINE

1. INTRODUCTION

The Central Bank of Barbados (Bank), in furtherance of its responsibility for the regulation and supervision of licensees under the Financial Institutions Act, 1996-16 and the International Financial Services Act, 2002-5 (IFSA), has developed this Guideline to provide guidance to licensees in relation to the Bank's expectations of their operational risk management practices.

The management of operational risk as a distinct risk category, similar to credit and market risk is a relatively new and growing area of risk management in the financial sector. Recent developments, including advances in technology, high profile operational loss events, greater use of outsourcing arrangements and the sheer size of some institutions have propelled the need for a strong operational risk culture.

The financial environment in Barbados is changing rapidly in response to some of these developments. Moreover, as licensees change ownership through mergers or outright buyouts, corporate structures and cultures will change. No significant operational losses in the sector have been reported, but the Bank requires that all licensees, regardless of size, implement an effective framework of policies and processes to identify, assess, monitor and control/mitigate operational risks as part of an overall approach to risk management.

This Guideline sets out the Bank's expectations in relation to the minimum standards for operational risk management by all licensees. It is based on the Basel Committee's guidance to the industry[1] and it will form the basis of the Bank's assessment of the effectiveness of the operational risk management framework of licensees.

The Bank recognises that there will be differences in approach by institutions. Licensees are expected to design a framework that satisfies the needs of their institution, taking account of its size and sophistication and the nature and complexity of its activities.

2. APPLICATION

This Guideline[2] on operational risk management applies to all entities that are licensed under the Financial Institutions Act 1996-16 (FIA) and IFSA of the laws of Barbados.

[1] Basel Committee (2003) "Sound Practices for the Management and Supervision of Operational risk".
[2] This guideline should be read in conjunction with the guidelines on Corporate Governance and Outsourcing.

The Bank recognises that some licensees are part of larger banking groups and may delegate some functions to their Head Office as part of their group wide risk management strategy. However, responsibility for compliance with the requirements of this Guideline remains with the licensee. Where licensees control a wider financial group, they must ensure that they implement procedures to ensure that operational risk is managed in an appropriate and integrated manner across the group.

3. OPERATIONAL RISK MANAGEMENT

The Basel Committee defines operational risk as:

> "The risk of loss resulting from inadequate or failed processes, people and systems from internal and external events."

It includes legal risk but excludes reputational and strategic risk. Operational risk is not generally taken in return for expected reward, but it may occur in the normal course of business activity. Due to the potential exposure to severe losses, the management of operational risk i.e. the identification, assessment, monitoring, and controlling/mitigating of risk is critical. Areas that should be captured in any operational risk management program include[3]:

a. Internal fraud;
b. External fraud;
c. Employment practices & workplace safety;
d. Clients, products & business practices;
e. Damage to physical assets;
f. Human losses;
g. Business disruption & system failures;
h. Execution, delivery & process management; and
i. Legal risk.

Consistent with the Guideline on Corporate Governance, the Board of Directors (Board) and Senior Management are responsible for developing an appropriate risk management environment within the institution. The Bank recognises that the risks faced by licensees and the practices used to mitigate risks may vary, but each licensee must ensure that it develops a framework that covers the full range of material operational risks it faces.

[3] See Appendix 1 for definitions of these risk areas.

3.1 Board Responsibility

The Board is ultimately responsible for the effective oversight of the licensee's operational risk management framework. The Board should:

i. Recognise that operational risk is a distinct and controllable risk present in virtually all transactions and activities of a licensee's operations;
ii. Be aware of the major operational risks faced by the licensee;
iii. Approve a firm wide operational risk strategy that:

   a. Provides a firm-wide definition of operational risk which should include legal risk;
   b. Reflects the licensee's tolerance for this risk as specified through the policies for management of this risk, including outsourcing risk;
   c. Outlines the policies for addressing the identification, assessment, monitoring and control of this risk;
   d. Establishes a management structure with specific lines of management responsibility, accountability and reporting to facilitate implementation of the strategy; and
   e. Creates a strong internal control culture in which control activities are an integral part of the regular activities of the licensee.

iv. Provide management with clear guidance and direction regarding the principles underlying the framework and to approve the corresponding policies developed by senior management;
v. Periodically review the framework to ensure that it meets the licensee's needs i.e. it encapsulates risk arising from market changes and other external factors as well as those associated with new products, activities or systems or other types of innovations as well as changes in industry. As part of the review process, the Board should update the framework to ensure that all material risks identified in its analysis are captured and that it incorporates the industry best practices for an entity of its size and operations;
vi. Receive reports that are sufficient to enable the Board to understand the licensee's overall risk profile and focus on the material and strategic implications for the business; and
vii. Ensure that the operational risk management programme is subject to an effective and comprehensive review by the internal audit unit. This includes:

   a. Ensuring the audit programme, scope and frequency is commensurate with the risk exposure; and
   b. Ensuring that the internal audit unit is not responsible for the operational risk management programme, thus enabling

independence of the audit function. The internal audit unit may assist in developing the program but responsibility for the day-to-day management must be transferred to another unit.

3.2 Senior Management

It is the responsibility of Senior Management to:

i. Implement the operational risk management framework approved by the Board. In doing so, senior management should:

   a. Develop policies, processes and procedures for managing risks in all of the licensee's material products, activities, processes and systems that can be implemented and verified within the different business units;
   b. Ensure the framework is consistently implemented throughout the entire organisation;
   c. Assign authority and responsibility and develop reporting relationships, which would encourage and maintain accountability. Reports from the various units should contain both internal and external market data and should provide adequate information to facilitate decision-making and motivate timely corrective action;
   d. Assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy and ensure that the necessary resources are available to manage operational risk effectively;
   e. Ensure that the licensee's operational risk management policy is clearly communicated to staff at all levels across all risk areas in units that incur material operational risks and that all level of staff understand their responsibilities with respect to operational risk management;
   f. Ensure that the licensee's staff have the necessary qualifications, experience, technical capabilities and access to resources, and that staff responsible for monitoring and enforcing compliance with the institution's risk policy have authority independent from the units they oversee;
   g. Ensure that policies, processes and procedures related to advanced technologies supporting high transactions volumes, in particular, are well documented and disseminated to all relevant personnel; and
   h. Ensure that remuneration practices are consistent with the licensee's risk tolerance and do not reward or encourage deviation or ignorance of policies as this can weaken risk management processes.

3.3 Internal Audit

Internal audit programs should be sufficiently robust and should verify that operating policies and procedures have been implemented effectively across the institution. Further, audit should periodically validate that the licensee's operational risk framework is being implemented effectively.

4. RISK MANAGEMENT: IDENTIFICATION AND ASSESSMENT

Risk identification is the first step towards the development of a viable operational risk monitoring and control system. Risk identification should include an analysis of all internal factors, such as structure, staff, activities and products, and external factors, such as technology advances, changes in the industry and other market information. Licensees are reminded that risk identification is not limited to an analysis of the factors identified but should be appropriate for the licensee's activities and level of sophistication. Moreover, a licensee may face significant operational exposure from product or activities that are not material to the business.

It is important that licensees:

i. Identify and assess the operational risk inherent in all material products, activities, processes and systems.
ii. 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.
iii. Make an assessment of their vulnerability to potentially adverse risks in order to better understand their risk profile and manage their resources more effectively.
iv. Have appropriate information technology policies and processes to address issues of information security and system development and that the level of technology expenditure is in line with the nature and complexity of its operations.

Licensees may develop their own set of risk management tools, but some possible tools that could be used for identifying and assessing operational risks are outlined in Appendix 2. Some exposures may not lend themselves to quantitative assessment and licensees may want to use relative estimates such as high, medium and low.

4.1 Risk Management: Monitoring

An effective monitoring process is essential for managing operational risk. It can assist in the early detection and correction of deficiencies and the prevention or reduction in the potential severity of a loss event. Licensees should:

i. Implement a system to monitor operational risk profiles and material exposures to losses on an ongoing basis;
ii. Incorporate regular reporting of operational exposures, loss experience and authorised deviations from the operational risk policy to senior management and the Board;
iii. Escalate on an exception basis unauthorised deviations, likely or actual breaches in thresholds for exposures and losses and significant increases in exposure to operational risk;
iv. Identify appropriate key risk or early warning indicators of an increased risk of future losses as part of the monitoring program. These 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, system downtime, and so on. Additionally, licensees should set appropriate thresholds (or risk tolerances) for these indicators, where possible;
v. Establish a monitoring frequency that reflects the degree of risk and nature of changes in the operating environment. Information from monitoring should be included in regular management and board reports;
vi. Require business units, group functions, the operational risk management unit and internal audit group to report to senior management on all areas of the operational risk within their preview. Reports should be distributed to appropriate levels of management and to business units within the institution where areas of concern may have an impact. These 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. Additionally, the reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues;
vii. Ensure that reports are analysed to facilitate improved existing risk management performance as well as developing new risk management policies, procedures and practices. Senior management may also use reports prepared by the external auditor, supervisory authority or other external source to assess the reliability and quality of internal reports. Further, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and the licensee's internal controls in general.

4.2 Risk Management: Risk Mitigation

The control and/or mitigation of operational risks are essential for effective operational risk management. Licenses should:

i. Establish policies, processes and procedures to control and/or mitigate material operational risks;

ii. Determine whether to use appropriate procedures to control and/or mitigate the risks, or to bear the risks. For those risks that cannot be controlled, licensees should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely;

iii. Establish control processes and procedures 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 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 authorisations to ensure accountability to an appropriate level of management.

iv. Develop an effective internal control system with appropriate segregation of duties. Personnel (or teams) should not be assigned responsibilities, which may create a conflict of interest. All areas of potential conflicts of interest should be identified, minimised, and subject to careful independent monitoring and review;

v. Complement segregation of duties with:

   a. Close monitoring of adherence to assigned risk limits or thresholds;
   b. Use of safeguards for access to, and use of, assets and records;
   c. Appropriate staff expertise and training;
   d. Identification of 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
   e. Regular verification and reconciliation of transactions and accounts.

vi. Use risk mitigation tools or programmes to reduce exposure to, or the frequency and/or severity of tail events (i.e. high severity, low probability operational risk events). For example, licensees may use insurance policies to protect against unforeseen operational risk events. Licensees should, however, view these risk mitigation tools or programmes as complementary to rather than a replacement for thorough internal operational risk control. Further, careful consideration should be given to assessing whether a risk mitigation strategy is truly reducing risk or is simply transferring it to another section of the business;

vii. Pay special attention to internal control activities when engaging in new activities or developing new products (particularly where these activities or products are not consistent with their core business strategies), entering unfamiliar markets, and/or engaging in businesses that are geographically distant from the head office;

viii. Invest in appropriate processing technology and information technology security. However, licensees 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 its immediate control (e.g., external events). Licensees should manage this risk by establishing appropriate business continuity and disaster recovery plans. These plans should be comprehensively documented and distributed;

ix. 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 specialised business activities. However, the use of third-parties does not diminish the responsibility of the licensee to ensure that the outsourced activity is conducted in a safe and sound manner and in compliance with applicable laws. Further guidance on the management of outsourcing risk is contained in the Bank's Guideline on Outsourcing;

x. Ensure that, if it opts to either retain a certain level of operational risk or self-insure against that risk, the decision to retain or self-insure the risk is transparent within the organisation and is consistent with the overall business strategy and appetite for risk; and

xi. Conduct periodic review of 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.

4.3 Business Continuity Management

Business Continuity Management is a significant aspect of operational risk management. Licensees should therefore develop policies, standards and procedures to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption caused by operational disruption, natural disasters, epidemics or terrorism.

Licensees should:

a. Identify the risks to 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;
b. Assess the potential impact of various disruption scenarios, including a major operational disruption, to which the organisation may be vulnerable, commensurate with the size and complexity of its operations;
c. Establish recovery objectives and priorities in the event of disruption. These objectives should be influenced by the likely impact of the disruption to the broader financial system;
d. Develop detailed business continuity plans for implementing the recovery strategy. This should include identification of 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 maintained at an off-site facility, or where 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 minimise the risk that both primary and back-up records and facilities will be unavailable simultaneously;
e. Develop communication strategies, in the event of a disruption, within the organisation and with relevant third parties, including regulators in other jurisdictions where a branch or subsidiary operates;
f. Review periodically their disaster recovery and business continuity plans so that they are consistent with the current operations and business strategies;
g. Test these plans periodically with all relevant personnel to ensure that the licensee would be able to execute the plans in the unlikely event of a severe business disruption; and
h. Subject these tests to audit review and address any deficiencies that are identified.

5. DISCLOSURE

Banks are encouraged to make sufficient public disclosure to allow market participants to assess their approach to operational risk management. The nature and frequency of disclosures should be commensurate with the size, risk profile and complexity of a bank's operations.

6. ROLE OF THE BANK

The Bank undertakes periodic inspections of a licensee's policies, procedures and practices, including those for operational risk management. Licensees should be aware that this examination is designed to provide an understanding of the licensee's practices and their effectiveness. The examination will inter alia include a review of:

i. The effectiveness of the licensee's risk management process and overall control environment with respect to operational risk, including that related to outsourcing and legal risk;
ii. The licensee's methods for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk;
iii. The licensee's procedures for the timely and effective resolution of operational risk events and vulnerabilities;
iv. The licensee's process of internal controls, reviews and audit to ensure the integrity of the overall operational risk management process;
v. The effectiveness of the licensee's operational risk mitigation efforts;
vi. The quality and comprehensiveness of the licensee's disaster recovery and business continuity plans;
vii. The licensee's information technology policies and processes to satisfy itself that areas such as information security and system development have been addressed and that the investment in information technology is commensurate with the size and complexity of their operations; and
viii. The licensee's process for assessing overall capital adequacy for operational risk in relation to its risk profile and, internal capital targets. While there is no current requirement to calculate regulatory capital for operational risk, it is expected that as part of its capital management programme, institutions will maintain adequate levels of capital to cover all risks including operational risk.

Licensees are required to incorporate into their quarterly report to the Bank all material adverse developments at their institution. All internal audit reports, as well as internal operational risk reports prepared for senior management and the Board should be copied to the Bank on request. Additionally, the Bank may solicit information on the licensee's operational risk management directly from the external auditors. All management letters from the external auditor should be forwarded to the Bank as soon as they are finalised.

All deficiencies identified by the regulator during the review process should be corrected. Licensees may be asked to submit an action plan acceptable to the supervisor to address deficiencies. Failure to address deficiencies may result in further supervisory action.

Appendix 1

Elements of an Operational Risk Management Programme

Internal Fraud

Internal fraud refers to unauthorised activity, theft or fraud that involves at least one internal party. Some examples of events that are classified as internal fraud include inter alia:

a. Intentional misreporting of positions;
b. Unauthorised undertaking of transactions;
c. Deliberate mis-marking of positions;
d. Insider trading (on an employee's own account);
e. Malicious destruction of assets;
f. Theft/robbery/extortion/embezzlement;
g. Bribes/kick-backs;
h. Forgery; and
i. Wilful tax evasion.

External Fraud

External fraud refers to theft or fraud carried out by a third-party outside the organisation. It includes, for example:

a. Theft/robbery;
b. Forgery;
c. Computer hacking damage;
d. Theft of information; and
e. Cheque kiting.

Employment Practices & Workplace Safety

This category refers to events relating to employee relations, a safe working environment and diversity/discrimination. Examples of events that could give rise to operational losses include:

a. Employee compensation claims (for example, diversity/discrimination events);
b. Wrongful termination;
c. Violation of health and safety rules;
d. Discrimination claims;
e. Harassment; and
f. General liability (for example, slip and fall events).

Clients, Products & Business Practices

Operational losses in this category arise from a failure to meet an obligation to a client, or from the nature or design of a product. Examples of events in this category include:

a. Breaches of fiduciary duties;
b. Suitability/disclosure issues;
c. Account churning;
d. Misuse of confidential client information;
e. Antitrust;
f. Money laundering;
g. Product defects; and
h. Exceeding client exposure limits.

Damage to Physical Assets

This category accounts for losses as a result of disasters and other events. It therefore includes:

a. Natural disasters (earthquakes, fires, floods, and so on);
b. Terrorism; and
c. Vandalism.

Human Resources

This includes the unavailability or loss of employees, including those providing outsourcing services to the licensees.

Business Disruption & System Failures

Operational event risks in this category include:

a. Hardware and software failures;
b. Telecommunication problems; and
c. Utility outages/disruptions.

Execution, Delivery & Process Management

This category covers risk events related to transaction processing or process management, trade counterparties and vendors. Examples of such events include:

a. Miscommunication;
b. Data entry errors (for example, wrong data, incorrect marking-to-market);
c. Missed deadline or responsibility;
d. Model/system misoperation;
e. Accounting errors;
f. Mandatory reporting failures;
g. Missing or incomplete legal documentation;
h. Unapproved access given to client accounts;
i. Non-client counterparty disputes;
j. Vendor disputes; and
k. Outsourcing.

Legal Risk

Legal risk is defined as the risk of unenforceable contracts (in whole or in part), lawsuits, adverse judgments or other legal proceedings disrupting or adversely affecting the operations or condition of a bank. Legal risk can arise due to a variety of issues, from broad legal or jurisdictional issues to something as simple as a missing provision in an otherwise valid agreement.

Losses due to legal risk depend on how the law allocates risk between the licensee and the other parties to a transaction, i.e. the extent to which the licensee has to bear losses not allocated to other parties. This can happen, for example, because a licensee may be deemed by the Courts to have failed to provide sufficient information to counterparties when selling them sophisticated (and/or tailor-made) products. Therefore, not only do losses due to legal risks depend on whether the risk event (contract breach, lawsuit, and so on) takes place, but they also depend on who will bear the loss if the event occurs.

Appendix 2

Risk Management Tools

Common risk management tools include:

i. **Self or Risk Assessment:** A licensee assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists, scorecards and/or workshops to identify the strengths and weaknesses of the operational risk environment.

ii. **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.

iii. **Risk Indicators:** Risk indicators are statistics and/or metrics, often financial, which can provide insight into a licensee's risk position. These indicators should be reviewed on a periodic basis to alert licensees to changes that may be indicative of risk concerns.

iv. **Measurement:** Some firms have begun to quantify and model their exposure to operational risk using a variety of approaches. For example, data on a licensee's historical loss experience could provide information for assessing its 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. Some firms have also combined internal loss data with external loss data, scenario analyses, and risk assessment factors.

These tools may be complemented by an assessment of risk indicators such as customer complaints, processing volumes, employee turnover, level of reconciling items, process or systems failures, etcetera.