Operational Risk Management Policy

Operational Risk Definition

A bank, including a development bank, is influenced by the developments of the external environment in which it is called to operate, as well as by its internal organization, procedures and processes. A bank faces mainly three types of risk: credit risk, market risk and operational risk.

Operational risk is defined 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. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

Operational risk can be created by a wide range of different external events ranging from power failures to floods or earthquakes to terrorist attacks. Similarly, operational risk can arise due to internal events such as the potential for failures or inadequacies in any of the bank's processes and systems (e.g. its IT, risk management or human resources management processes and systems), or those of its outsourced service providers. Operational risk arising from human resources management may refer to a range of issues such as mismanaged or poorly trained employees; the potential of employees for negligence, willful misconduct; conflict of interests; fraud; rogue trading; and so on. Therefore the emergence of mistrust, failure to communicate, low morale and cynicism among staff members, as well as increased turnover of staff, should be regarded as indicative for potential increase in operational risk.

Operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process.

Types of Operational Risk Relevant to BSTDB

Operational risk event types having the potential to result in substantial losses include:

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

- External fraud. For example, robbery, forgery, cheque kiting, and damage from computer hacking.

- Employment practices and workplace safety.

- Disregard of Bank policies, strategies, guidelines, rules and regulations, as well as inappropriate or ineffective use of existing control mechanisms by Bank personnel in relation to a particular client, or attempts to create "shortcuts" in order to advance personal agendas.

- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the Bank's account, money laundering, and sale of unauthorised products.

- Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.

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

- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

Main Factors Generating Operational Risk

The events mentioned above may occur due to both internal and external factors in the following areas:

A Internal factors

1 People

The management of human resources and employees behavior can become a major source of operational risk. Poorly trained or overworked employees may inadvertently expose the Bank to operational risk (for example, via processing errors). Understanding of the mandate, confidence in and respect for the institution as well as adherence to the Bank's policies and strategies are key for effective use of human resources. In addition, the continuous availability of its employees, or the Bank's ability to replace them, can influence its ability to recover from interruptions to the continuity of its operations. Therefore, the Bank can realize significant improvements in its control of operational risk and reduce exposure if it would invests time and money in creating an appropriate risk culture, in which employees are aware of operational risks and are encouraged to learn from their mistakes.

2 Processes and systems

Bank's operations are supported by many different systems and processes, such as IT systems, human resource management systems, credit, market, insurance and liquidity risk management systems and even operational risk management systems.

These systems may have many different components, each of which require the operation of various processes. For example, the credit risk management system of the Bank should and does include processes for the identification, measurement, monitoring and control of credit risk.

Complex or poorly designed systems and processes can give rise to operational losses, either because they are unfit for purpose, or because they malfunction. As a result, the Bank may experience a wide range of problems, including settlement-processing errors, fraud and information security failures. In addition, the increasing automation of systems and our reliance on IT has the potential to transform risks from minor manual processing errors to major systematic failures.

B External factors

External events can have a major impact on a firm. The Bank should be aware that both expected and unexpected changes to its operations can be major sources of operational risk. The Bank should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness.

1. Disruptive events

Such events include fire, flooding, earthquakes, terrorist actions, vandalism, power failures, etc. The Bank should assess the potential risk for such events to happen, design and put in place disaster recovery systems and procedures, with a view to ensuring continuity of activity. Against the monetary loss derived from such events the Bank should evaluate potential cost and acquire proper insurance.

2. Use of Consultants and Outsourcing of Services

Outsourcing arrangements require careful management if they are to yield benefits, and where they are not managed adequately the degree of operational risk faced by the Bank may increase, as is also the case of excessive use and dependency upon the use of consultants for activities that may be more effectively developed internally. In particular, an issue for concern is the loss of control over processes. This could create a serious threat to the continuity of its operations if these providers were to fail.

Responsibilities

The Board of Directors shall be aware of the major aspects of the Bank's operational risks as a distinct risk category that should be managed, and it shall approve and periodically review this framework. It shall ensure that the Bank's operational risk management framework is subject to effective and comprehensive internal audit, as mentioned in the Key Processes below.

Senior Management shall have responsibility for implementing the operational risk management framework approved by the Board of Directors. The framework should be consistently implemented throughout the Bank, and all levels of staff shall understand their responsibilities with respect to operational risk management. Senior Management shall also ensure that the necessary policies, processes and procedures for managing operational risk in all of the Bank's material products, activities, processes and systems are in place.

Compliance and Operational Risk Management Office shall have responsibility according to its Charter, approved by the BoD.

BSTDB's appetite and tolerance for operational risk

BSTDB has a low appetite and tolerance for material operational risks it is exposed to. Therefore, all appropriate measures will be taken towards achieving a high level of operational risk awareness and the establishment of a rigorous operational risk management system.

Principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated

BSTDB's Operational Risk Management Framework:

i) Clear strategies adopted by the Board of Directors and oversight exercised by Senior Management (the President, Vice-Presidents and the Secretary General),

ii) Strong internal operational risk culture (Internal operational risk culture is taken to mean the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management) and internal control culture, emphasizing on dual controls,

iii) Effective monitoring and internal reporting,

iv) Contingency and business continuity plans,

v) High standards of ethics and integrity, and

vi) Commitment to effective corporate governance, including, among others, segregation of duties, avoidance of conflicts of interest, and clear lines of management responsibility, accountability and reporting, as reflected in the Bank's corporate governance documents. All levels of staff shall understand their responsibilities with respect to operational risk management.

Key processes for the management of operational risk:

The establishment of the Compliance and Operational Risk Management Office itself is deemed to contribute to the improvement of the management of the Bank's operational risk. Among others, the Office shall regularly perform operational risk monitoring activities, in order to promptly detect deficiencies in the policies, procedures and processes, and propose corrective actions. The frequency of monitoring shall reflect the risks involved and the frequency and nature of changes in the operating environment.

The scope and breadth of the activities of the Compliance and Operational Risk Management Office shall be subject to independent periodic review by the Internal Audit Department, as described in the Charter of the Compliance and Operational Risk Management Office. Administrative Services Department and Information Technology Department are responsible for the infrastructure and logistical support of the contingency planning of the Bank, each on its area of competency. Reporting lines between above operational risk control units shall be established in order to avoid conflicts of interest.

All units of the Bank shall conduct self-assessment exercises of the specific operational risks inherent in their activities, including their identification and assessment with regard to their frequency of occurrence and materiality, and shall report the identified events to Compliance and Operational Risk Management Office. During the risk identification process consideration shall be given to both internal factors (such as the Bank's structure, the nature of the Bank's activities, the quality of the Bank's human resources and human resource management, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the Bank's objectives. For all identified material operational risks, for which no control mechanisms are in place, the Bank shall decide whether to create such mechanisms, or bear the risks. The timely reporting of operational losses and their prompt addressing by the competent management shall be fostered.

Key risk indicators shall be developed, where appropriate, to act as early warnings of increased risk of potential losses. Effective tracking of these indicators by the Compliance and Operational Risk Management Office shall allow the Bank to identify changing risks upon their occurrence and respond to them promptly.

During a New Products Approval process the operational risk related to each new product, activity, process and system, or their amended versions, will be identified and assessed, and mitigating controls will be established.

Insurance policies may be used to confront losses which may occur as a result of events such as third-party claims resulting from errors and omissions, employee or third-party fraud, and natural disasters.

Disaster recovery and business continuity plans shall take into account different types of plausible scenarios to which the Bank may be vulnerable, commensurate with the size and complexity of the Bank's operations. Such plans shall periodically be reviewed and tested.

With regard to the adequacy of the human resources, all efforts shall be made to ensure that staff has appropriate expertise and training. Also, adequate performance assessment systems and career advancement procedures should be in place.