Charter of the Compliance and Operational Risk Management Office (CORMO)

Compliance Risk

Compliance risk is defined as the risk of legal sanctions, material financial loss, or loss to reputation the Bank may suffer as a result of its failure to comply with laws, its own regulations, code of conduct, and standards of best/good practice.

Compliance risk is sometimes also referred to as integrity risk, because a bank’s reputation is closely connected with its adherence to principles of integrity and fair dealing.

As per the Basel Committee on Banking Supervision “The compliance function should have a formal status within the bank to give it the appropriate standing, authority and independence. This may be set out in the bank’s compliance policy or in any other formal document. The document should be communicated to all staff throughout the bank.”

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.

According to the Basel Committee, an Operational Risk Management system must be implemented by an independent and distinct operational risk management function.

Establishment of the Compliance and Operational Risk Management Functions

The Bank gives paramount importance to identifying, measuring and mitigating risks inherent in its activity. To this end, the revised Financial Policies of BSTDB place high importance on a Comprehensive Risk Management system, stating that: “The Bank is committed to actively identify and manage all risks inherent in its activities in order to support its sustainable profitability objective and safeguard its capital base. The Bank pays particular attention to managing credit risks in the course of its core activities and treasury operations, market risks in its Treasury as well as compliance and operational risks in its organization and activities.”

In the 40th Board of Directors Meeting, held in September 2004, the Bank approved the Organization Structure of the Bank, which included two new functions within the Internal Audit Department, namely the Compliance Risk Management and Operational Risk Management functions.
As per decision 0406-41-BD2004-80 of BSTDB’s Board of Directors taken on 6 December 2004 “The compliance function within the Bank –as approved by the Board in September 2004 through the newly adopted Organization Structure document– should be separated from the audit function of the Bank and compliance risk should be included in the risk assessment methodology of the internal audit function. A compliance policy should be presented for adoption by the Board, providing for the above-mentioned separation of functions, defining responsibilities and reporting arrangements to the Board. Its implementation should be the responsibility of the management.”

**Status of the Compliance and Operational Risk Management Office – Reporting Relationships**

The Compliance and Operational Risk Management Office is a unit independent of the business activities of the Bank. However, a co-operative working relationship between Compliance and Operational Risk Management Office and business units shall be established to identify and manage compliance and operational risks at an early stage.

The Office is reporting to the President of the Bank and the Board of Directors, through its Chairman, on the Bank’s compliance and operational risk management efforts.

Representatives from each of the Bank’s Divisions and operating units, as appointed by the respective Directors or Heads of the units with the approval of the respective supervising member of the Senior Management, at the Head of the Compliance and Operational Risk Management Office’s request, shall assist from time to time the Head of the Compliance and Operational Risk Management Office in carrying out his responsibilities in areas of their expertise.

Specific tasks of the Compliance and Operational Risk Management Office requiring technical skills not available within the Bank or of confidential nature may be outsourced, in conformity with the Bank’s applicable rules and regulations, however, provided the outsourcing arrangement is overseen by the Head of the Compliance and Operational Risk Management Office who maintains full and final responsibility for the entire activity of the Office.

**Resources of the Compliance and Operational Risk Management Office**

The resources to be provided for the Compliance and Operational Risk Management Office shall be both sufficient and appropriate to ensure that the respective risks within the Bank are managed effectively. In particular, the Office’s staff shall have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties. Their professional skills shall be maintained through regular and systematic education and training.

**Role of the Office**

The Compliance and Operational Risk Management Office performs two sets of activities/functions:
a. Assists Senior Management in managing effectively the compliance risks faced by the Bank. To this end, it identifies, assesses, advises on, monitors and reports accordingly on the Bank's compliance risk,
b. Assists the Bank in managing the operational risk. The office shall identify, assess, monitor and control/mitigate the operational risk inherent in all material products, activities, processes and systems.

Authority granted to the Compliance and Operational Risk Management Office

The Head of the Compliance and Operational Risk Management Office has direct authority to exert control over the entire compliance and operational risk management process performed by the Office, from program design to enforcement. All activities of the organization other than internal audit are to be subject to regular compliance and operational risk management reviews and testing in accordance with the annual compliance and operational risk management programs.

Under the guidance of the President the Head of the Compliance and Operational Risk Management Office has the right to i) conduct special investigations in relation to the Office’s responsibilities, ii) request for contribution to such investigations from other units of the Bank, as per their expertise, and iii) appoint outside experts, if appropriate.

On every compliance and operational risk management assignment, with the exception of the Internal Audit Department, the accountable management is expected to allow unrestricted right of access to the Compliance and Operational Risk Management Office staff: on its own initiative to communicate with any staff member and obtain access to any records or files necessary to enable it to carry out its responsibilities. For assignments of a confidential nature the President’s permission only with regard to access rights will be sought.

Documents and information given to compliance and operational risk management officers are handled in the same prudent manner as by those employees normally accountable for them.

Management is responsible for controls and risks and for action to correct deficiencies in systems of control.

Main Responsibilities

a. Compliance Risk Management function main responsibilities
   • On a pro-active basis, to identify, document and assess the compliance risks associated with the Bank’s business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships;
   • To assist senior management in educating staff on compliance issues in coordination with the Human Resources Department which shall assist in facilitating the training/education;
• To assist and advise the business groups and the Credit Committee on operations related integrity and reputational issues, including -among others- checks on borrowing clients, project sponsors and other partners, upon request;

• Under the guidance of the President the Head of the Compliance and Operational Risk Management Office shall lead and co-ordinate investigations into alleged unsatisfactory conduct or misconduct of Bank employees or consultants, and, where appropriate, recommend disciplinary or corrective action;

• To deal with and lead and co-ordinate investigations into issues of conflict of interest (of the Bank, staff, etc), cases of alleged corruption, money laundering, terrorist financing, and complaints received with regard to Bank-financed operations;

• To consider ways to measure compliance risk and use such measurements to enhance compliance risk assessment;

• To assess the appropriateness and consistency of the Bank’s regulatory framework (statutory documents, policies, strategies, guidelines, rules, regulations and procedures in force) related to compliance issues, promptly following up any identified deficiencies in the policies and procedures and, where necessary, formulating proposals for amendments;

• To ascertain compliance with the provisions of the Bank’s Code of Conduct, to review and propose amendments to the Bank’s Code of Conduct and other policies and procedures, as necessary, to reflect ethical standards in all areas;

• The responsibilities of the compliance function shall be carried out under a risk based annual compliance program that sets out its planned activities, subject to oversight by the head of compliance to ensure appropriate coverage and co-ordination among risk management functions.

• To report on a regular basis to the President of the Bank and the Chairman of the Board of Directors. The reports shall refer to the compliance risk assessment and testing which has taken place during the reporting period, any identified breaches and/or deficiencies, the corrective action taken; any compliance matters that should be brought to their attention for information or action purposes, and shall contain information about compliance training provided to compliance function and other bank staff;

Compliance responsibilities carried out by staff in different units are allocated among the units as per their expertise. A close co-operation will be established between the Compliance and Operational Risk Management Office and such units with respect to the provision and exchange of relevant advice and information and the cumulative reporting of the compliance risks.
b. Operational Risk Management function main responsibilities

- To review the Bank’s policies and procedures and place operational risk within the Bank’s overall risk management and strategic framework, thereby enhancing and promoting the Bank’s risk and control awareness culture.

- To implement and maintain the Bank’s operational risk monitoring and control system, including also the regular monitoring of operational risk profiles and material exposures to losses, and detecting and making proposals for the correction of deficiencies in the related policies, procedures and processes. To report regularly pertinent information, including recommendations made, to the President of the Bank and the Chairman of the Board of Directors that support the proactive management of operational risk.

- To quantify operational risk for the Bank’s activities as necessary, according to best standards and practices utilizing internationally accepted methodologies.

- To advise the banking teams and other staff on operational risk matters and facilitate reporting of relevant risk information up, down and across the Bank by framing accountability and authority for operational risk management in the business units.

- To deal with and lead and co-ordinate investigations into cases of internal and external fraud;

- To participate in the new products approval process, in order to identify and assess the operational risk related to each new product, activity, process and system, or their amended versions, to be introduced or undertaken, and present operational risk mitigation proposals.

Relationship with the Internal Audit Department

The scope and breadth of the activities of the Compliance and Operational Risk Management Office are subject to independent periodic review by the Internal Audit Department. Compliance and Operational risks are included in the risk assessment methodology of internal audit. The review of compliance and operational risk management activities by internal audit consists of assessing the controls in place to ensure that all relative risks are adequately mitigated according to best practices and the Bank’s policies and procedures; the establishment and effective functioning of the Compliance and Operational Risk Management Office consists such a control.

The Internal Audit Department, according to the Bank’s Internal Audit Charter and other relevant policies and procedures, will keep the Head of Compliance and Operational Risk Management Office informed of any significant audit findings relating to compliance, as appropriate. Respectively, the Head of Compliance and Operational Risk Management Office will also keep the Internal Audit Department informed of significant findings in relation to compliance and operational risk control deficiencies.
Every effort will be made to enable communication and coordination between the Compliance and Operational Risk Management Office and the Internal Audit Department, aiming at ensuring appropriate coverage of these areas and avoidance of overlapping of tasks or responsibilities.

Relationship with other risk management functions

Every effort will be made to enable communication and coordination between the compliance and operational risk management functions, and credit risk management and Assets & Liabilities Management functions in relation to issues of compliance and operational risk management, aiming at ensuring appropriate coverage of these areas and avoidance of overlapping of tasks or responsibilities.