Disclosure related to Operational Risk Management

Bank of India, Hong Kong branch, Operational Risk Management Policy has been framed to create an enabling organisational culture and place a high priority on effective operational risk management and implementation of risk management processes. The Policy has been drafted considering various regulatory guidelines issued by HKMA and the Basel Committee on Banking Supervision from time to time.

The operational risk management policy at the head office describes the approach to Operational Risk Management within the Bank as part of Enterprise-wide Risk Management and also to comply with the regulatory guidelines. It outlines the Operational Risk Management Framework and describes the roles and responsibilities of the Board, the Risk Management Committee of the Board, and the Operational Risk Management Cell. It describes the process of risk identification, risk measurement, risk monitoring, risk categorisation, risk mitigation, risk reporting and capital measurement.

The Operational Risk Management Policy aims to improve the management and mitigation of operational risks across the Bank and to comply with Basel and HKMA requirements.

Organisational Setup and Key Responsibilities for Managing Operational Risk

Operational risk is intrinsic to a bank, and its management shall be an important component of the enterprise-wide risk management systems of the bank. The organizational culture shall give high priority to effective operational risk management and adherence to sound operating procedures. The organizational setup for operational risk management shall include the following:

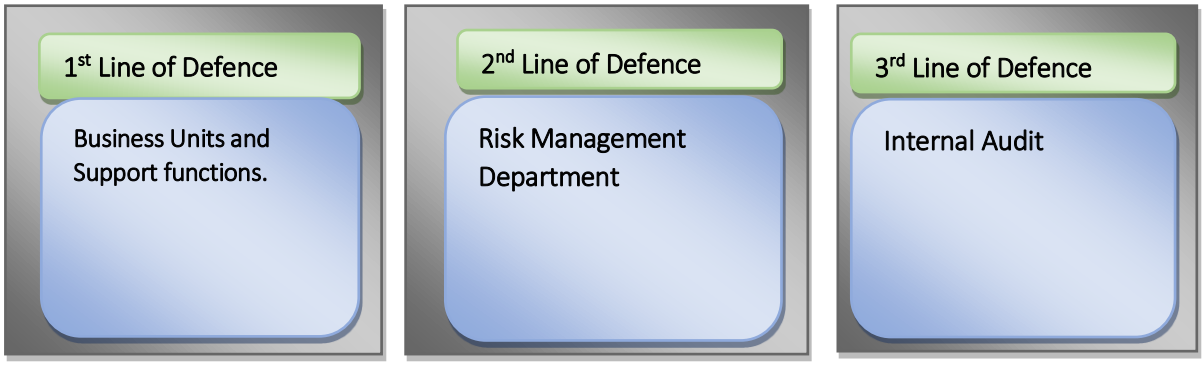
At the Bank (Head Office) level:

The Bank has adopted an integrated approach to risk management. Risk Management is a Board-driven function in the Bank. At the apex level of the risk management apparatus, there is a Board-level Risk Management Committee. At the operational level, a full-fledged Risk Management Department, headed by a Chief General Manager (Chief Risk Officer) with a complement of qualified and trained staff, is in place. The Bank also has separate Committees of top executives for managing various risks, viz.

- Market Risk Management Committee (**ALCO**) for management of market risk;
- Head Office Level Credit Committee (**HLCC**) for management of credit risk
- Committee for Operational Risk Management (**CORM**) for management of operational risk.

To manage Operational Risk across various products and processes, the Bank has adopted a '**three lines of defence**' risk governance model. The first line of defence is the role of Business Units and Support functions, while the second line and third lines of defence are the role of the Risk Management department and Internal Audit.

The risk governance model as adopted by the Bank is given below:



Roles of three lines of defence:

1st Line of Defence: BUSINESS UNITS / SUPPORT FUNCTION	2nd Line of Defence: RISK MANAGEMENT DEPARTMENT	3rd Line of Defence: INTERNAL AUDIT
Develop, implement and maintain operations and IT infrastructure and processing.	Develop and implement Operational Risk Management process, e.g. identification, measurement, monitoring process of Operational Risk etc.	Evaluate Operational Risk Management processes and framework, as part of the audit process.
Perform periodic RCSA exercise, track KRIs and identify and report loss data.	Develop, maintain and support RCSA, KRI and Loss data process. Develop and update Operational Risk framework of the Bank and related policies, procedures and methodologies.	Provide assurance on the reporting quality of data for KRI, RCSA and loss data. Use RCSA outcomes as a starting point for audit. Share audit findings with Risk Management Department.
Develop and implement approved action plans and controls for risk mitigation.	Develop and propose control standards; support implementation process.	Evaluate control effectiveness as part of audit process.

Risk Identification:

Risk identification is of paramount importance for the development of viable operational risk monitoring and control frameworks. Effective risk identification considers both internal factors (such as the complexity of the bank's structure, nature of activities, and quality of human resources, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of Bank's objectives. Based on past experience, the following operational risks have been identified at the Hong Kong Centre level.

- **People Risk** – Placement, Competency, work environment, motivation, turnover/rotation
- **Process Risk** - Transaction risk, transaction guidelines, errors in the execution of transactions, product complexity, competitive disadvantage
- **Systems Risk**-Technology Risk- System failure, system security, programming error, communications failure, MIS Risk.

The Operational Risk which is inherent in them is to be adequately assessed for mitigation of risk. Control measures against each risk are also to be clearly defined. The Bank, along with new products/process assessments, would primarily use the Risk and Control Self-Assessment (RCSA) to identify, evaluate, monitor and mitigate key operational risks within the Bank.

The objective of the RCSA process is to:

- Identify key Operational Risks across various products and processes within the Bank;
- Assess the risks that matter in various businesses, products and processes;
- Assess the design and the effectiveness of internal controls;
- Prioritize the control improvement initiatives to manage the Operational Risk profile of the Bank;
- Develop (more effective) alternative controls for the unacceptable risks; and
- Assist in embedding Operational Risk Management process in day to day activities of the Bank.

Key steps involved in conducting the RCSA exercise would include:

- Identification and assessment of risks based on severity and probability of Operational Risk.
- Identification and assessment of control design and operating effectiveness
- Arriving at the residual risks and
- Formulation of an action plan for the gaps identified and for risks beyond the tolerance level of the Bank.

Risk Measurement:

The bank has instituted a structured process for reporting operational risk incidents on a regular basis**.** Each Business unit must ensure that the Operational Risk Incident data are submitted to the Operational Risk Management System (system capable of collecting and processing data collected from various sources and reporting the same) and that the required data meets all established standards for timeliness and integrity.

The operational Risk Management cell would treat an event as a significant incident under the conditions.

1. Events constituting loss above the set threshold.
2. Incident which seriously jeopardises the business operations (for example, system downtime, strike, etc.)
3. Incidents caused/causing threat to employee life.

Monitoring of Operational Risk

An effective and regular monitoring process is essential for adequately managing operational risk and offers the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment and shall be decided while finalising the events to be tracked. The reports on these monitoring activities, as well as the compliance reviews performed by the internal audit functions, shall be included in regular reports to the Risk Management Committee.

The operational risk reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision-making and taking corrective measures. Reports should be analysed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

For the purpose of operational risk management, the activities of the bank have been divided into the following eight business lines identified in the New Capital Adequacy Framework –

1. Corporate finance
2. Trading and sales
3. Retail banking
4. Commercial banking
5. Payment and settlement
6. Agency services
7. Asset management
8. Retail brokerage

All activities of our bank at Hong Kong Centre are mapped into the above eight levels.

Risk Mitigation

Risk management is the process of mitigating the risks faced by a bank. With regard to operational risk, several methods may be adopted for mitigating the risk. For example, losses that might arise on account of natural disasters can be insured against. Losses that might arise from business disruptions due to telecommunication or electrical failures can be mitigated by establishing backup facilities. Loss due to internal factors, like employee fraud or product flaws, which may be difficult to identify and insure against, can be mitigated through strong supervisory and internal auditing procedures.

Insurance, collateral, and backup are some of the most commonly used risk mitigants. In some instances, the bank may decide to either retain a certain level of operational risk or mitigate the risk. Where this is the case and the risk is material, the decision to retain or mitigate the risk should be transparent within the organisation and should be consistent with the bank's overall business strategy and appetite for risk.

- For all material operational risks that have been identified, the Centre shall decide whether to use appropriate procedures to control and/or mitigate the risks or bear the risks. For those risks that cannot be controlled, the bank shall decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

- Classification of operational risk events into various risk categories (high, low, medium) based on severity, frequency and such events to be controlled and tracked.

- Investment in appropriate processing technology and information technology security are also important for risk mitigation, though increased automation could transform low severity-high frequency losses into high severity-low frequency losses like loss or extended disruption of services caused by internal factors or external events beyond the bank's immediate control.

- The centre has in place contingency disaster recovery and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. The centre also has a DR site for business continuity purposes.

- The bank periodically reviews the disaster recovery and business continuity plans so that they are consistent with the bank's current operations and business strategies. Moreover, these plans are tested periodically to ensure that the bank would be able to execute the plans in the unlikely event of a severe business disruption.

- Based on Loss event data and severity-frequency analysis, the Risk Management Committee shall initiate further mitigation and control measures wherever considered necessary.