Board Paper No : 2024 / 742 / 06 / J **Date : 28 / 06 / 2024**

Board Meeting No : 74

OPERATIONAL RISK MANAGEMENT POLICY & PROCEDURES

Policy Owner	**: Chief Risk Officer**
BIRMC Presented Date	**: 14 / 05 / 2024**
Board Approved Date	**: 28 / 06 / 2024**
Version	**: 01**

Table of Contents

1 Introduction

Operational Risk is intrinsic to financial institutions and it should be an important content of an organization-wide Risk Management framework. Fnance Companies with a strong culture of Risk Management are less likely to experience potentially damaging Operational Risk events and are better placed to deal effectively with thoseevents that do occur. This policy outlines the Internal operating policies of LCB Finance's Operational Risk Management Framework. The document sets out a context that complies with the regulatory requirements towards managing Operational Risk.

The policy provides guidance on the Management of Operational Risks and Controls by adequately identifying, assessing, monitoring and reporting different types of Operational Risks including Information Technology (IT) Risk and establishing controls to mitigate the losses arising from the risks.

Operational Risk Management Unit will review this document annually or prior to the annual review based on any internal or regulatory requirements.

This policy will be approved by the Board of Directors while the Board Integrated Risk Management Committee (BIRMC) of the LCBF would be responsible for the oversight of implementation of this policy.

1.1 Objective of Operational Risk Management

1. **Establishing Clear Accountability**: Ensure that senior management at LCBF is held accountable and responsible for effectively managing operational risks within their respective areas of oversight.
2. **Fostering Common Understanding**: Develop a shared understanding of operational risk acrossall business and operational units within the LCBF. This enables accurate assessment of exposure to operational risks and facilitates the implementation of appropriate risk mitigation measures.
3. **Enhancing Internal Controls**: Improve internal controls throughout the LCBF to mitigate the probability and potential impact of losses resulting from operational risk incidents. Strengthening internal controls helps to safeguard the LCBF's assets and reputation.
4. **Establishing a Risk Loss Database**: Create and maintain a comprehensive database to collect and monitor operational risk-related lapses and losses. This facilitates the identification of trends, enables proactive risk management strategies, and supports continuous improvement efforts.
5. **Ensuring Regulatory Compliance**: Meet the regulatory requirements set forth by regulatory bodies such as the Central Bank of Sri Lanka, Securities and Exchange Commission, and Companies Act. Adherence to regulatory guidelines helps to mitigate regulatory risks and maintain the LCBF's reputation and standing in the financial industry.

All employees are required to read, understand, and comply with the requirements that have been set out herein. Business / Operations Heads are responsible to ensure that all staff under their purview have read and understood the policy.

2 Definition of Operational Risk

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 Strategic and Reputational Risk.

Operational Risk is relevant to every aspect of the Company's business and covers a wide spectrum of issues. Losses arising through fraud, unauthorized activities, errors, omission, inefficiency, systems failure or from external events all fall within the Operational Risk definition. IT Risks arise due to IT related events that could potentially impact business and customers. It can occur with both uncertain frequency and magnitude and may create challenges in meeting goals and objectives of the LCBF. Management of Operational Risk related to IT Risks would be covered in detail under the different security standards and specific policies for IT related activities issued from time to time.

BASEL III Definition of Operational Risk

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

- **Internal Process Risk** – In a Finance Company refers to the potential risks associated with the company's internal operations, systems, and processes. These risks can arise from deficiencies or weaknesses in the processes, which may lead to operational failures, financial losses, regulatory issues, or reputational damage.
- **People Risk** – In a Finance Company refers to the potential risks associated with the company's employees, including their actions, behaviors, competence, and overall effectiveness in carrying out their roles within the organization.
- **System Risk** - In a Finance Company refers to the potential risks associated with the company's information technology (IT) systems and infrastructure. These risks stem from vulnerabilities, failures, or disruption in the company's IT systems, which can have significant consequences for the company's operations, financial stability and reputation.

Types of Technology Risk

- Access Risk – Information may be divulged to unauthorized recipients
- Availability Risk – Service may be lost or data may not be accessible
- Cyber and Information Risk – Faliure to safeguard privacy, confidentiality, integrity, and availability of information
- Emerging Technology Risk – Threats associated with new technology
- Infrastructure Risk – IT infrastructure may be unable to support business needs
- Integrity Risk
- Investment or Expense Risk

- **Eternal Event Risk** - In a Finance Company refers to the potential risks arising from events or circumstances outside the company's control that can impact its operations, financial performance, or reputation. These events are typically disasters, geopolitical events, economic downturns, regulatory changes, and other external factors.

2.1 Operational Risk Governance Structure

The organizational chart for Operational Risk Management is presented below. These roles and responsibilities relate only to the activities relating to Operational Risk Management. The composition and Terms of Reference of the Board Integrated Risk Management Committee (BIRMC) and Executive Integrated Risk Management Committee (EIRMC) would be defined in the Integrated Risk Management Policy of the Company.

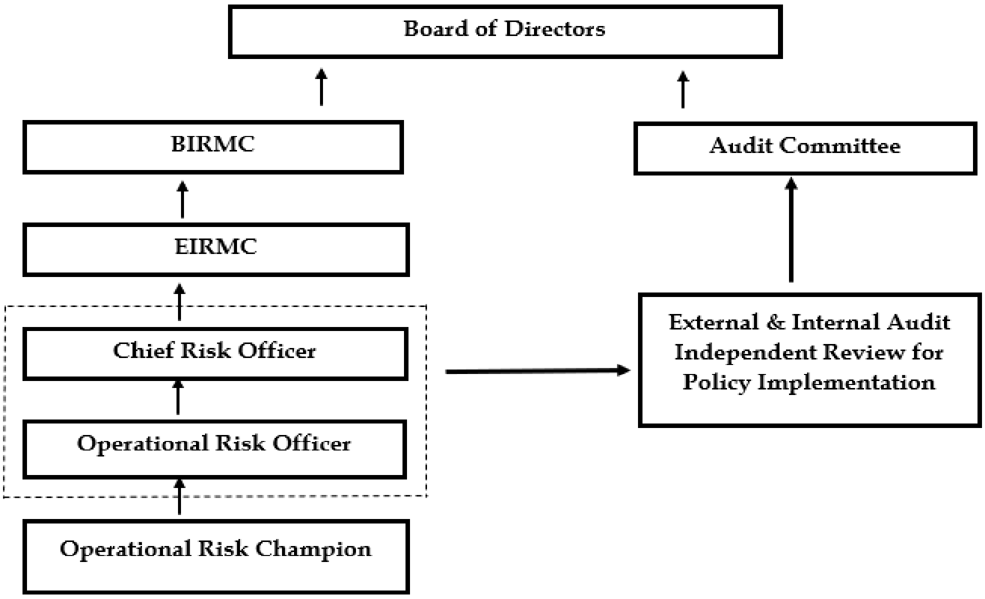
Board of Directors
BIRMC
Audit Committee
EIRMC
Chief Risk Officer
Operational Risk Officer
External & Internal Audit Independent Review for Policy Implementation
Operational Risk Champion

Figure 1 Operational Risk Governance Structure

2.1.1 Key Functions & Roles of the Board of Directors and BIRMC

1. **Setting LCBF-wide Strategies:**

The Board of Directors is responsible for approving operational risk strategies that provide a clear management structure. This includes aligning these strategies with the overall business goals and risk appetite of the Company.

2. **Policy and Framework Oversight:**

The Board and BIRMC review and approve the Operational Risk Management policy and framework, ensuring they are comprehensive, effective, and aligned with regulatory requirements. Regular yearly reviews are conducted to adapt to evolving risks and industry standards.

3. **Defining Risk Appetite:**

The Board establishes the risk appetite for operational risk, indicating the level of risk the LCBF is willing to accept to achieve its objectives. This guides decision- making at all levels of the organization and helps manage risk within predefined boundaries.

4. **Capital Methodology Approval:**

The approval of the operational risk capital methodology and the resulting attribution is a crucial function. This involves determining the amount of capital required to cover potential losses associated with operational risk, ensuring financial resilience.

5. **Cultural Reinforcement:**

The Board and BIRMC play a pivotal role in fostering a culture of operational risk awareness and management throughout the organization. This includes promoting a mindset where every employee understands and actively contributes to identifying, assessing, and mitigating operational risks.

6. **Monitoring and Oversight:**

Both the Board and BIRMC have a responsibility to monitor the effectiveness of operational risk management practices. They receive regular reports on risk exposures, incidents, and the overall risk profile, ensuring that the Company's risk management efforts align with strategic objectives.

7. **Regulatory Compliance:**

Ensuring compliance with regulatory requirements related to operational risk management is a critical role. The Board and BIRMC stay informed about changes in regulations, assess their impact on the Company, and take necessary actions to maintain compliance.

8. **Communication and Transparency:**

The Board and BIRMC communicate operational risk strategies, policies, and key decisions transparently to stakeholders. This includes providing insights into the LCBF's risk position and the effectiveness of risk management practices.

9. **Emergency Response and Crisis Management:**

In the event of significant operational risk events or crises, the Board and BIRMC are involved in decision-making and crisis management. They may establish crisis response teams and ensure the implementation of contingency plans to mitigate the impact of the crisis.

10. **Training and Development:**

The Board and BIRMC may support training initiatives to enhance the capabilities of employees in understanding and managing operational risks. This helps in building a skilled workforce capable of navigating the complexities associated with operational risk

2.1.2 Key Functions and Roles of the Chief Risk Officer

1. Oversee the implementation of policies, processes and procedures for managing Operational Risks established under the operational risk framework.

2. **Authority and Responsibility Assignment:**

The CRO assigns authority and responsibility to identified resources within the organization to manage operational risks effectively in their respective functions. This ensures that risk management responsibilities are clearly defined and understood throughout the organization.

3. **Communication of Strategies and Policies:**

The CRO ensures that the LCBF's operational risk strategies, policies, and management expectations are clearly communicated to staff at all levels. This facilitates alignment with organizational objectives and promotes a culture of riskawareness and accountability.

4. **Facilitating Communication:**

The CRO facilitates adequate communication between operational staff and those involved in risk management functions. This ensures that relevant risk information is effectively communicated, enabling timely decision-making and risk mitigation efforts.

5. **Review of ORM Reports:**

The CRO reviews the Operational Risk Management (ORM) reportsof the respective business units on a regular basis, typically monthly or quarterly. This involvesanalyzing risk indicators, incidents, and trends to assess the effectiveness of risk managementpractices and identify areas for improvement.

6. **Analysis of Operational Risk Losses:**

The CRO reviews and analyzes operational risk losses at business units falling under the purview of respective senior management. This analysis helps identify root causes of losses, assess their impact on the organization, and implement corrective actions to prevent recurrence.

7. **Exposure Assessment Monitoring:**

The CRO monitors the qualitative and quantitative assessment of exposure to all types of operational risks faced by the business units. This involves evaluating risk metrics, stress testing results, and scenario analyses to understand theorganization's risk profile and inform risk management decisions.

8. **Control Implementation:**

The CRO ensures that adequate controls and systems are put in placeto identify and mitigate risks before they become major concerns. This includes implementingrisk monitoring tools, establishing control mechanisms, and continuously assessing the effectiveness of risk mitigation efforts.

2.1.3 Key Functions and Roles of Operational Risk Officer

1. **Policy Development:** Draft specific operational risk policies, standards, procedures, andguidelines to manage the operational risk cycle (identify, measure, monitor, and control). Seekapproval from the Board of Directors or other appropriate authority to ensure alignment with organizational objectives and regulatory requirements.

2. **Policy Maintenance:** Regularly update operational risk policies and procedures as needed to reflect changes in business operations, industry standards, and regulatory requirements. Ensurethat policies remain relevant and effective in addressing evolving operational risks.

3. **Risk Analysis:** Analyze operational risks associated with all existing and new products launched by the LCBF. Assess potential risks and develop strategies to

mitigate them, ensuring that risk considerations are integrated into product development processes.

4. **Documentation:** Document operational risk management policies, procedures, and communication protocols. Ensure that relevant staff are aware of and adhere to these policies, fostering a culture of risk awareness and compliance throughout the organization.

5. **Tool Development:** Identify and develop tools for the management of operational risks, such as risk assessment methodologies, key risk indicators (KRIs), and risk monitoring systems. Implement tools to enhance risk management capabilities and improve decision-making processes.

6. **Framework Enhancement:** Undertake enhancements to the operational risk framework to adapt to changing business environments and emerging risks. Continuously evaluate the effectiveness of risk management practices and make necessary adjustments to strengthen theframework.

7. **Risk Limits Establishment:** Establish operational risk limits, including KRI thresholds and losslimits. Seek approval for these limits and monitor adherence on an ongoing basis. Report regularly on risk exposures and exceptions to management and relevant stakeholders.

8. **Risk Assessments:** Facilitate Risk and Control Self-Assessments (RCSA) periodically to identify high, medium, and low risks across the LCBF. Collaborate with business units to assessand prioritize risks, and develop action plans to mitigate identified risks.

9. **Data Tracking:** Ensure uniform and consistent tracking of operational risk data, including losses and near misses, across the LCBF. Maintain accurate records of risk incidents and use data analysis to identify trends and areas for improvement.

10. **KRI Monitoring:** Periodically monitor Key Risk Indicators (KRIs) across business units and follow up on exception plans initiated to mitigate identified risks. Take proactive measures toaddress breaches of KRIs and prevent potential risk incidents.

11. **Control Adequacy Review:** Review the adequacy of controls to manage overall operational risks associated with business activities. Identify control weaknesses and recommend enhancements to mitigate operational risk exposures effectively.

12. **Fraudulent Cases Review:** Review and report significant fraudulent cases and lapses in controlto senior management and relevant stakeholders. Implement measures to strengthen fraud prevention and detection mechanisms.

13. **Insurance Policy Review:** Review and analyze the adequacy and coverage of insurance policies to mitigate operational risks. Determine optimal insurance limits

and ensure that insurance coverage aligns with the LCBF's risk tolerance and business objectives.

14. **Culture and Awareness Building:** Foster an operational risk-aware culture across the LCBF by promoting awareness of operational risk management principles and practices among staff. Conduct training sessions and communication campaigns to enhance risk awareness and promote accountability.

15. **Risk Champion Meetings:** Conduct regular meetings with risk champions to discuss critical issues, non-compliance with ORM policies, and key risk management issues. Collaborate withrisk champions to address concerns and implement effective risk management strategies.

2.1.4 Key functions and Roles of Operational Risk Champion

Each Business/Operations unit/ Branches at the LCBF would appoint officials to be designated as Operational Risk Champions for management of Operational Risk in their respective departments/ branches.

The Operational Risk Champions would report to Operational Risk Management Officer for the Operational RiskManagement activities. The main responsibilities of an Operational Risk Champion would include:

1. **Design and Collection of Risk Indicators:** Actively participate in the design, collection, and reporting of risk indicators relevant to their respective departments or branches. Collaborate with stakeholders to ensure comprehensive coverage of operational risk indicators.
2. **Timely Reporting of Loss Events:** Ensure timely collection and reporting of loss events, including IT incidents, within their business units or branches. Report such events to the Operational Risk Management Unit in accordance with established reporting protocols.
3. **Risk and Control Self - Assessment (RCSA):** Facilitate and participate in risk and control self-assessment (RCSA) exercises within their units. Verify the results of the RCSA process and identify areas for improvement or corrective actions.
4. **Action Plan Documentation:** Timely follow-up and documentation of the status of action plansdeveloped to address gaps or issues identified during RCSA exercises. Ensure that action plansare implemented effectively to mitigate identified risks.
5. **Design and Collection of Key Risk Indicators (KRIs):** Actively participate in the design, collection, and data capture of key risk indicators (KRIs) relevant to their respective groups ordepartments. Ensure that KRIs are meaningful, relevant, and aligned with operational risk objectives.
6. **Monthly Reporting:** Regularly report loss data, near-miss data, and KRIs to the Operational Risk Management Unit on a monthly basis. Provide accurate and timely information to facilitate effective monitoring and management of operational risks at the organizational level.
7. **Communication and Collaboration:** Foster a culture of risk awareness and

accountability within their units or branches. Communicate operational risk management policies, procedures, and expectations to staff members and encourage active participation in risk management activities.

8. **Continuous Improvement:** Identify opportunities for enhancing operational risk management practices within their units or branches. Propose recommendations for process improvements,risk mitigation strategies, or control enhancements to mitigate operational risks effectively.
9. **Training and Development:** Provide training and guidance to staff members on operational risk management principles, practices, and tools. Promote awareness of risk management bestpractices and encourage staff involvement in risk identification and mitigation efforts.
10. **Coordination with Operational Risk Management Officer:** Maintain regular communication andcollaboration with the Operational Risk Management Unit. Seek guidance and support as needed to address complex risk issues or challenges encountered within their units or branches.

3 Risk Categorization

In order to provide clarity and a common language around Operational Risk Management, the LCBF would classify Operational Loss events into two primary categories.

Loss Events: The actual occurrence of Operational Risk events would be categorized into one of "Actual Loss", "Near Miss" or "Potential Loss".

1. **Causes:** Each risk event is required to be mapped to the underlying cause and control that failed or permitted a risk/loss. More than one cause may be assigned to one loss event. The four major cause categories of Operational Risk are briefly described below:

- Process – the risk resulting from inadequate or failed internal processes.
- People – the risk resulting from the deliberate or unintentional actions or inadequate understanding/ knowledge of activity, training, etc.
- Systems – the risk resulting from inadequate or failed system infrastructure including network, hardware, software, communications and their interfaces.
- External – the risk resulting from events outside of the LCBF's direct or indirect control or from events that may impact an external relationship. For example, external frauds, floods,earthquake and other natural calamities.

The LCBF would use loss event categories as the primary risk classification methodology.

The event categories will be used to organize Operational Risk analysis across self- assessment, loss database,capital calculation and reporting tools. All Operational Risk or incidents will be assigned to one event category. There are many potential causes that could contribute to the occurring of a risk or incident.

4 Three Lines of Defense in the Basel Model

First Line of Defense – Business line management is responsible for identifying and management risks

- Inherent in products, activities, processes and systems
- Accountable for their management

Second Line of Defense –

Responsibilities of the Risk and Compliance

- Measuring the operational risks
- Establishing the reporting processes for operational risks
- Establishing the risk committees to measure and monitor operational risks
- Reporting operational risk issues to the Board of Directors

Key Functions

- Challenging the business lines' risk management activities
- Ensuring alignment with the company's risk management and reporting framework

Third Line of Defense –

Company's audit function performs independent oversight of the first two lines

- Auditors mut not be participants in the process under review
- Review can be conducted by external party
- Independent review team reports to Audit Committee on internal control, compliance and governance

5 Fundamental Principles of Operational Risk Management

5.1 Risk Culture

Strong risk management culture spearheaded by the company's board of directors and senior managers

- Provide a sound foundation for a strong risk management culture within the company
- Less likely to experience potentially damaging operation risk events
- Better placed to deal effectively with the outcome of such an event

Establish a code of conduct for all employees

- Outlines expectations for ethical behavior
- Identifies acceptable business practices and prohibited conflicts

Provide risk training throughout all levels of the company

- Takes into account the level of seniority, roles, and responsibilities of the trainees

5.2 Board Oversight

Establish a culture and processes for understanding operational risks - Includes board members, managers, and employees

- Regularly review the framework for emerging / evolving risks
- Provide senior management with guidance and approve policies

- Ensure independent review by skilled personnel
- Follow evolution of best practices
- Establish strong internal controls with clear and responsibilities

5.3 Operational Risk Appetite

Operational Risk appetite is the acceptable maximum level of risk that the LCBF is willing to accept in pursuitof its business objectives. Operational Risk appetite is primarily aimed at creation and management of a robust risk culture in the LCBF.

The level of Operational Risk losses as a percentage of Net Operating profit and/or Equity of the LCBF shouldbe "Low", "Moderate" or "High" as defined below:

The levels of Operational Risk losses are "Low", "Moderate", and "High".

The thresholds for operational losses for "Low", "Medium" and "High" would be defined through the RiskAppetite Statement (RAS) at the annual budgeting and RAS process.

The qualitative risk appetite based on operational loss event type is given below.

Loss Event Types	Qualitative statement for Risk Appetite
1. Internal Frauds	Zero tolerance for losses due to acts of a type intendedto defraud, misappropriate property or avoid regulations, law or LCBF policy, which involves at leastone internal party.
2. External Frauds	Low appetite for losses due to act of a type intended to defraud misappropriate property or avoid laws, by a third party external to the LCBF.
3. Employment Practices and Workplace safety	Zero appetite for losses arising from acts inconsistent with employment, health or safety laws or agreementsfrom payment of personal injury claims, from diversity/discrimination events, from business disruptions.
4. Client's products & Business Practices	Zero risk appetite for losses arising from an unintentional or negligent, failure to meet a professional obligation to specific clients or from the nature or design of a product.
5. Damage to Physical Assets	Low appetite for loss arises from loss or damage to physical assets from natural disaster or other events.
6. Business Disruption & System Failures	Low appetite for business disruptions /system failuresfor more than stipulated SLAs'/ Downtimes. CBSL Direction No. 01 of 2022 Technology Risk Management & Resilience effective 01.01.2023 LFCs shall

	ensure the availability of DR arrangements for critical information systems with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) determined by the Board of Directors on the recommendation of BIRMC, confirming to following minimum requirements: i. RTO of less than 6 hours for critical information systems of LFC, and ii. RTO of zero (i.e. no data loss during a disaster) or near zero
7. Execution, Delivery & Process Management	Low appetite for losses from failed transactionprocessing or process management.

6 Operational Risk Management framework

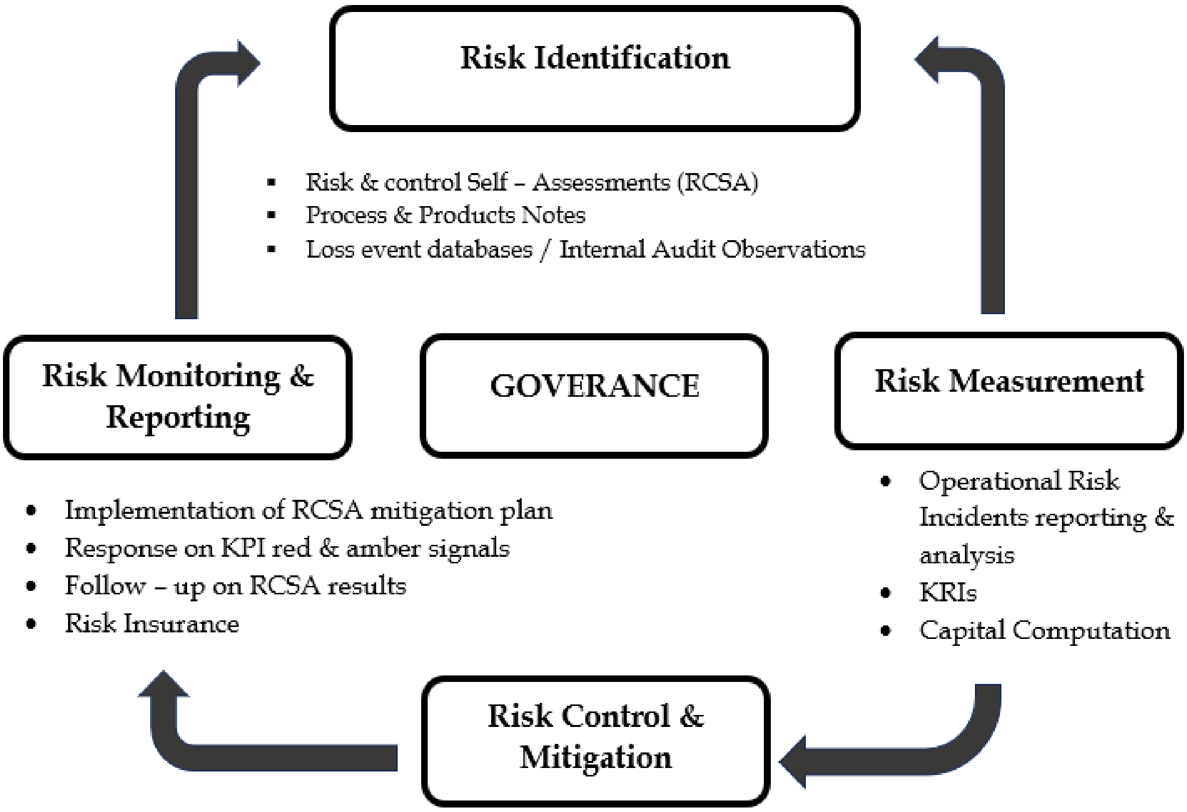
Risk Identification
Risk & control Self – Assessments (RCSA)
Process & Products Notes
Loss event databases / Internal Audit Observations
Risk Monitoring & Reporting
GOVERANCE
Risk Measurement
Implementation of RCSA mitigation plan
Response on KPI red & amber signals
Follow – up on RCSA results
Risk Insurance
Operational Risk Incidents reporting & analysis
KRIs
Capital Computation
Risk Control & Mitigation

Figure 2 Operational Risk Management framework

6.1 Risk Identification

Risk and Control Self-Assessment (RCSA) is a methodology of assessment of Operational Risks in all the products and processes in terms of identifying and understanding potential Operational Risks in the LCBF.

It is a process of self-assessment by the business/ process owners in each respective business/ operational department facilitated by Operational Risk Management Unit. The RCSA's can be either first time or on-goingrisk assessments.

The following define the operational procedure in conducting a RCSA activity in the LCBF.

6.1.1 Risk and Control Self-Assessment (RCSA) methodology

First time Risk assessments:

The assessment is done in two steps:

1. The products and processes are assessed for inherent risks and
2. Assessment of effectiveness of existing controls to arrive at the residual risks.

6.1.1.1 Assessment of Inherent Risk

The first step in the process is to identify and document the list of products/processes to be coveredfor a particular Business/Operations unit. This is done after referring to the list of approved product & process notes or office instructions that are in place. If there are no written documents in place, then the existing work flows and activities would be listed out by the particular Business/ Operationsteams.

Activities and what can go wrong (Risk) in each activity without considering the existing controls pertaining to the Business units is compiled by Risk Champion attached to the Business Unit after referring to the day today activities carried out by them, loss data, audit reports, audit checklist, policies and any other relevant documents.

The draft list is sent to Operational Risk Management Unit (ORMU) for review.

Thereafter, Operational Risk Officer will provide guidance to the Business Unit in identifying the inherent risks. The risks are to be identified in the template provided by the Operational Risk Officer. The inherent risk would be measured based on the

- Likelihood of impact
- Consequences of impact/ magnitude of impact

6.1.1.2 Assessment of Residual Risk

After the Business Unit agrees on the inherent risks in each activity in terms of both likelihood and magnitude of impact, then they would list down the existing controls in place for each activity/ process. The controls are to be measured in terms of control effectiveness as measured through;

1. Control Design
   a) Monitoring mechanism (who executes and monitors the control)
   b) Whether it is preventive or detective and control frequency
   c) Whether manual or IT/ System driven

2. Operating Environment (Frequency of past control breaches)

The rating scales would be designed and decided by the Operational Risk Management Unit.

Once the control effectiveness is agreed by the participants, a draft report on RCSA would be prepared by the Risk Champion of the Business Unit and reviewed by Operational Risk Officer.

The mitigation plan is also developed, during the preparation of draft RCSA with time lines and responsible persons. The draft report including the Operational Risk rating should be circulated by Operational Risk Officer to the members of the Executive Integrated Risk Management Committee (EIRMC).

Feedback received from the members of the EIRMC; should be incorporated by Operational Risk Officer in the report and the draft report is finalized and circulated to Chief Risk Officer (CRO) for review and sign-off.

The results of the RCSA are presented for review to the Chief Executive Officer (CEO) with the participation of the process owners and Risk Management unit. After review by the Senior Management, summary of the results would be presented to the BIRMC through CRO.

6.1.2 Monitoring of mitigation plans:

The Operational Risk Officer should follow-up on the status of completion of the mitigation plans as agreed by the process owners within the agreed timelines and any deviations to be reported to the respective Unit Head, CRO and CEO. If there are any extension of timeline for closure required, those should be documented and presented to the CRO and CEO. CRO to present these deviations tothe EIRMC and BIRMC along with justifications and extension of timelines.

6.1.3 Review of risk assessments on an on-going basis:

The plan for review of carrying out risk assessments on an on-going basis shall be prepared based onthe RCSA results for each Business/ Operational unit. For any units with high and significant risk the review should be semi-annually and for other units the review should be annually.

On an on-going basis, Operational Risk incidents (including IT related events, health & safety events,external disruptions, compliance and fraud events, if any) shall be mapped to the risks in the existingrisk assessment report. When there are indications of a significant changes in risk profile based on identified risk incidents, a full review of the Risk and Control assessment should be immediately carried out by the process owners and Operational Risk management unit. A summary report shall be presented to the EIRMC on the incidents not identified as risks at the initial RCSA for information and updates. The mitigation plans are also need to be presented.

On an on-going basis, any new regulatory guidelines impact the processes and changing the risk profile shall be considered for reviews and re-assessed by incorporating the changes in the risks. Any new product launch or major changes in the processes or implementation of new system / majorenhancements in the existing systems may be considered for inclusion in the plan for risk assessmentswhich would warrant a review of the risk assessments.

The methodology and approach adopted for the risk assessment for the first time shall be followed for reviews also.

6.2 Key Risk Indicators

Key Risk Indicators (KRIs) are tools used to monitor either exposure to key risks (on an inherent or residual basis) or controls for key risks. Examples of KRIs might include the number of system outages/ down times, staff turnover (increase/decrease) rate etc.

KRIs are to be established for each key risk for the overall business to ensure timely awareness. Formal escalation triggers, when a KRI reaches a critical level, may also be appropriate in certain cases. If a KRI cannot be established for a key risk, or for an associated control, an exception to this requirement may be agreed between business/operation department and Risk Management Department. The exception and its rationale must be documented and presented to the BIRMC.

To the extent possible, KRIs should recognize both improvement and deterioration in Operational Risk exposures on a timely basis, provide forward-looking information and translate risks into quantitativemeasures that lend themselves to verification.

KRI's would be:

1. Statistics and/or metrics which can provide insight into the risk position of the LCBF. The trends of the indicators will be reviewed on a monthly basis to alert the LCBF to changes that may be indicativeof risk concerns.
2. Appropriate indicators provide early warning of an increased risk of future losses. Thresholds will bedirectly linked to these indicators. The results of these monitoring activities will be presented to EIRMC on a monthly frequency. This will indicate the risk profile of the particular business group andhelp Senior management in taking timely corrective actions.
3. KRIs in majority of instances are designed for high and significant risks as identified in the RCSA process.
4. After the indicators are identified, threshold limits for the same are decided. Threshold levels are to be defined after taking the risk appetite of each business group and studying the historical data whereapplicable.
5. All the thresholds determined will be divided into 3 zones i.e. Red, Amber & Green.
    - Red zone denotes immediate action.
    - Amber zone indicates that action plan has to be drawn so as to prevent process / activity fromturning Red.
    - Green zone would indicate that the controls are working efficiently or in an acceptable manner.
6. For critical/zero tolerance indicators, there would be only two zones i.e. Red and Green. (e.g. Regulatory compliance related indicators normally have zero tolerance)
7. The threshold/tolerance limits are discussed by the Risk Champions and Risk

Management Dept. Theindicators along with the threshold limits shall be signed off with the respective business or operations head.

8. Primary responsibility of data collection for KRIs would be with the Risk Champions.
9. Once data is collected the same would be reported the EIRMC. Risk Management Dept. would consolidate and present the red and amber KRIs at the quarterly BIRMC meeting along with any mitigations that have been undertaken or proposed for corrective action.
10. For Red & Amber indicators, trend needs to be monitored. Based on the analysis of these trends for both Red and Amber indicators, mitigation plans should be put in place.
11. The Key Risks, Indicators and Threshold limits shall be reassessed on a yearly basis or on need basis after analyzing the trends of KRIs.

6.3 Risk Measurement and Incident Management

Operational Risk Incident:

Any event leading to Operational Risk either actual or potential is an Operational Risk event or incident. These incidents need to be reported as per regulatory requirement and they also help in taking corrective measures to prevent future re-occurrences.

Operational risk incidents can be classified in three categories;

1. **Actual Loss**: A Financial loss that results in a profit and loss movement within the reported financial year.

Examples:

- Communication to the customer for promising erroneous interest rate on loan/deposits.
- Compensation to the customer for wrongful execution of an instruction.

2. **Potential Loss**: An Operational Risk (OpR) incident with no immediate impact but where a futurefinancial loss is probable.

Examples:

- Erroneous commitment made in respect of a loan for which loss would be adjusted in future installments.
- Issuance of credit products without adequate / appropriate acceptance from the client leading that may result in mis-use and subsequent legal claim by the client.

3. **Near Miss**: An Op Risk incident where normal controls did not work as anticipated but a direct impact(financial loss) has been avoided.

Examples:

- Credit of funds given to a wrong customer, however, the mistake is identified immediately and corrective entries are passed by debiting the wrong customer and crediting back the correct customer. Here, there is no financial loss.

- Pay order prepared for a wrong amount however, the same is cancelled before handingover to customer and correct draft is prepared and issued.

Inclusions and exclusions in Operational Risk incidents:

1. Inclusions: Any cost involved to recover an Operational Risk loss would be included in Operational Risk. This may include any additional cost/overheads to recover the loss, compensation paid to the customer on account of the error by the LCBF, etc.
2. Exclusions – Any compensation to the customer as a service gesture would be excluded (i.e. for incidents wherein LCBF is not at error.)

The above list is indicative in nature and incidents beyond the scope of this should also be considered.

6.4 Mapping of loss events to Business lines

The Business line mapping establishes a process whereby the activities of the LCBF are first identified and then mapped to the regulatory business lines in accordance with the requirements of Basel II accord, the revised guidelines on Computation of Risk-weighted Amount for Operational Risk by the CBSL All operationalrisk losses will be categorized into the defined 8 Business Lines.

Business Line		**Activity Groups**
Level 1	**Level 2**	
Corporate Finance	Corporate Finance Government Finance Merchant LCBF	Mergers and acquisitions, underwriting, privatizations, securitization, research, debt (Government, high yield), equity syndications, IPO, secondary private placements.
Trading & Sales	Sales Market Making Proprietary Positions Treasury	Fixed income, equity, foreign exchanges, credit products, funding, own position securities, lending and repos, brokerage, debt, prime brokerage and sale of Government bonds to retail investors.
Payment and Settlement	External Clients	Payments and collections, inter - LCBF funds transfer (RTGS, EFT etc.), clearing and settlement
Agency Services	Custody	Escrow, securities lending (customers) corporate actions, depository services
	Corporate Agency	Issuer and paying agents
Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open,private equity

	Non - Discretionary FundManagement	Pooled, segregated, retail, institutional, closed, open
Retail Brokerage	Retail Brokerage	Execution and full service
Retail LCBF	Retail LCBF	Retail lending and deposits, LCBF services, trust andestates.
	Private LCBF	Private lending (personal loans) and private (institutional) deposits, LCBF services, trust and estates, investmentadvice.
Commercial LCBF	Commercial LCBF	Lending including project finance, corporate loans, real estate, trade finance including export and import loans, letter of credit, bills of exchange, leasing, factoring and guarantees. Institutional deposits and other repayable funds.

Any operational loss incident would be mapped into the seven loss events types (described in section 4 above) and eight business lines. ORMU would present the summary to the EIRMC and BIRMC on a monthly/ quarterlybasis.

6.5 Loss data capturing frame work

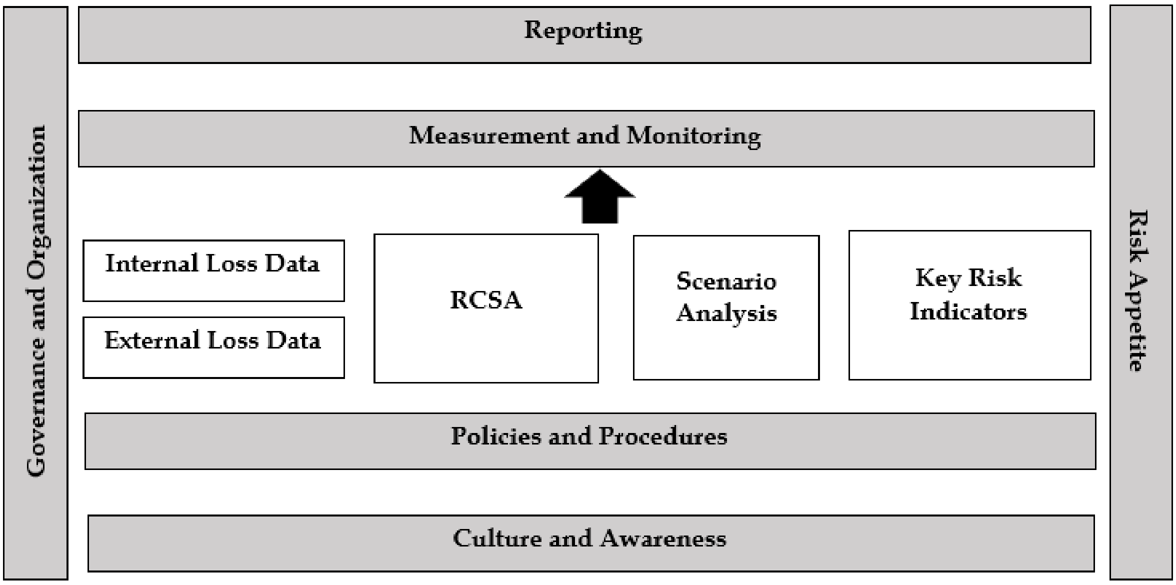

Figure 3 Loss data capturing frame work

Internal Controls – LCBFs should adopt well-established internal control systems, which include segregation of duties, clear management reporting lines and adequate operating procedures in order to mitigate operational risks. Corporate Governance (Prevailing Direction No. 05 of 2021) for licensed LCBFs: (a) a report by the Board should be included in the Annual Reporton the LCBF's internal control mechanism that confirms that the financial reporting system has been designedto provide reasonable assurance regarding the reliability of financial reporting and that the preparation of financial statements for external purposes has been done in accordance with relevant accounting principles and regulatory requirements; and (b) the external auditor's certification on the effectiveness of the internal control mechanism referred to in (a) above, in respect of any statements prepared or published. A proper internal control system should: (a) promote effective and efficient operation; (b) provide reliable financial information; (c) safeguard assets; (d) minimize the operating risk of loss from irregularities, fraud and errors; (e) ensure effective risk management systems; and (f) ensure compliance with relevant laws, regulations andinternal policies.

7 Reporting

7.1 Reporting Requirements

All business/operations units must report all Operational Risk related incidents i.e. Actual Losses, Potential Losses, Near Misses **IMMEDIATELY** in the internal incident report format through the respective Line Management/ Unit Operational Risk Champion to Operational Risk Management Unit (ORMU) and Chief RiskOfficer (CRO).

Operational Risk related lapses (where there is no Actual Operational Loss, Potential Loss or a Near miss) mustalso be reported to CRO, Manager Operational Risk via respective Line Management in the same internal incident report format. Operational Risk related incidents must be informed to CEO and The BIRMC as appropriate through Chief RiskOfficer.

In case, where the loss amount is not determinable at the time of recording, employee will record a provisional estimate of the loss amount, if any. The employee can intimate ORMU to amend the provisional amount subsequently.

Recovery against financial loss will be entered while reporting the loss event, if such recovery is made at the point of reporting. In case recovery is made later, the same needs to be informed to ORMU to update the database.

An operational loss event can also be identified through the investigation analysis of the financial ledger by external auditors, internal auditor and regulator, or customer complaints triggers.

7.2 Root Cause Analysis (RCA) of Operational Risk Incident / Event

Post identification of Operational Risk event and capturing in the required template, each business/ operations unit should prepare a summary report for review of the incident and the necessary corrections being made to the Risk Management Dept.

The respective Operational Risk Champions should submit detailed Root Cause Analysis (RCA) reports (as per the template given by Risk Department) for the critical activities along with mitigations of all Operational Riskincidents to ORM Unit within two weeks of the incident taking place which will be reviewed by the ORM Unitto ensure complete information has been analyses and disclosed. ORMU will then update the Operational Risk Events for further analysis and to maintain a complete log of therisk events happened covering the entire LCBF. For larger Operational Risk incidents, ORMU should carry outan independent RCA. The identified and reported risk incidents and the Root Cause Analysis would be reported by IRMD to the EIRMC and BIRMC along with the mitigation plans and timelines.

The respective Operational Risk Champions of business/ operational units would track mitigations for all Operational Risk incidents for closure which would be monitored by the ORM Unit. Any delays in implementing mitigations should be reported to ORM Unit with proper justifications. Any such delays wouldbe reported to the CEO and the EIRMC with revised timelines.

7.2.1 Incident Reporting system

The incident reporting system in the LCBF serves as a crucial mechanism for identifying and addressingoperational risks promptly. Here's an elaboration on how it operates:

1. Risk champions, appointed in each branch, business unit or department, play a vital role in incident reporting. They are responsible for promptly reporting any identified incidents or potentialrisks to the incident reporting system.
2. These champions are typically individuals who have a deep understanding of the operations withintheir respective units and are well-positioned to recognize and assess potential risks.
3. The incident reporting system is designed to be accessible to all employees within the organization.This ensures that every staff member, regardless of their role or level within the hierarchy, has the ability to report incidents they observe.
4. By granting access to all employees, the LCBF encourages a culture of accountability and risk awareness throughout the organization. It empowers every individual to contribute to the riskmanagement process by promptly reporting any incidents or concerns they encounter.
5. Every employee within the LCBF has a responsibility to report any incidents or risks they observethrough the incident reporting system.
6. This responsibility extends beyond risk champions to include all staff members, from frontline employees to senior executives. It emphasizes the importance of collective vigilance and proactiverisk identification across the organization.
7. Incident reporting should occur in real-time or as soon as the incident is identified. Promptreporting ensures that potential risks are addressed swiftly, minimizing their impact on theorganization's operations and reputation.
8. Employees are encouraged to report incidents without delay, following established protocols andprocedures outlined in the incident reporting system.
9. The incident reporting system should guarantee confidentiality and protection against

retaliationfor employees who report incidents in good faith.

10. Employees should feel safe and supported when reporting incidents, knowing that their concernswill be taken seriously and addressed appropriately by the organization.
11. The incident reporting system should also facilitate continuous improvement by capturing data onreported incidents. This data can be analyzed to identify trends, recurring issues, or areas of concern, allowing the organization to implement preventive measures and enhance its risk management practices over time.

Overall, the incident reporting system serves as a critical tool for fostering a culture of risk awareness, transparency, and accountability within the LCBF, with every employee playing a role in identifying andmitigating operational risks

7.3 Reporting to the Risk Committees

Operational Risk Management Unit will be receiving below details from respective Business units on monthlybasis and reporting the same to EIRMC on monthly basis and BIRMC on quarterly basis.

Once we completed the Risk and control Self Assessments (RCSA) Process; we will report the departmentspecific Key Risk Indicators (KRIs) to Risk Committees.

No	Item	Received by	Reporting Frequency
1	Key Risk Indicators - Department Specific	EIRMC / BIRMC	Monthly / Quarterly
2	Key Risk Indicators - Company - wide	EIRMC / BIRMC	Monthly / Quarterly
2	Operational Losses (Incidents & Amounts)	EIRMC / BIRMC	Monthly / Quarterly
3	Fraud cases (Incidents & Amounts)	EIRMC /BIRMC	Monthly / Quarterly
4	Summary Root Cause Analysis of Ops Risk Incidents,Mitigations and timelines	EIRMC /BIRMC	Monthly / Quarterly
5	Errors/ Failures of Digital Transactions and Trends	EIRMC /BIRMC	Monthly / Quarterly
6	Customer Complaints (Type & Trends)	EIRMC /BIRMC	Monthly / Quarterly
7	Error adjustments done by Efinance system operetion unit	EIRMC /BIRMC	Monthly / Quarterly
8	Outstanding Audit Observations/ Issues	EIRMC /BIRMC	Monthly / Quarterly

7.4 Escalation Process

The IRM Department would escalate to CEO, EIRMC, BIRMC and BoD any material Operational Risk incidents/ Losses.

I. Any material Operational Risk incidents and Losses above Rs. 100,000/- along with the root cause analysis and mitigation plans with timelines for closure.

II. KRI's within Amber Zone (refer section 5.2 above) and the trend of deterioration if any.

III. KRIs' within the Red Zone and the action plan for rectification

IV. Any material deviations to agreed workarounds/ mitigation action plans (as defined in the RCSA process and/ or for operational risk incidents) with justifications and/ or extension of timelines for closure. The material deviations to mitigations and extensions for timelines for closure should be approved by the BIRMC.

8 Risk mitigation

Risk mitigation is a critical element in the Risk Management framework. Following are the key elements and procedures pertaining to Operational Risk mitigation:

1. Primary mitigation comes through the implementation of the action points emanating from the Risk and Control Self Assessments (RCSAs), Operational Risk incidents analysis, red and amber key risk indicators.
2. Mitigation plans should contain the timelines and person responsible for implementation of the plan.
3. ORMU should ensure that the status of overdue mitigation actions in respect of high and significant risks,red and amber indicators and major incidents is reported to the EIRMC on a monthly basis and BIRMC on a quarterly basis.
4. Extension of timelines in respect of mitigation actions, if any, shall be approved by the BIRMC.
5. ORM Unit should also participate in the annual insurance policy renewal assessment exercise carried outby the Administration and Finance departments. During the annual review, the ORM Unit shall ascertainif any of high, un-mitigated operational risks can be insured
6. In case some of the significant and high risks are not covered by the existing insurance policy, the concerned business/ operational unit shall analyze the cost benefit of taking an insurance cover and consider obtaining such insurance cover.

9 Management of Information Technology Risks

Management of IT risks is an important component of the LCBF's operational risk management framework, and it comprises IT governance, a continuous technology risk management process, implementation of sound practices in respect of IT controls, cyber security and ensuring quality of the IT and Digital systems. In additionto the following IT Risk covered in ISMS – Information Security Management System Manual according to theBaseline Security Standard for Information Security Management.

1. The Company will integrate the risk management processes for the LCBF's electronic LCBF activities into its overall IT risk management approach. There shall be an effective management oversight over the risks associated with electronic LCBF activities, including specific accountability, policies and controls to manage them.
2. The Company shall have a Policy regarding Information Security and ensure that it is

regularly reviewed and updated.

3. The Company will have appropriate measures to ensure adherence to customer privacy requirements as mandated by CBSL and other regulatory bodies as appropriate.
4. The Company will have appropriate procedures to comply with legislative, regulatory and contractual requirements on the use of systems and software as applicable.
5. The Company will have a comprehensive and centralized change control system so that all changes are appropriately reviewed and approved.
6. The Company will have an appropriate programmed and project management to all IT projects for managing project risks. A consistent and formally defined programmed and project management
7. approach shall be applied, that enables stakeholder participation and monitoring of project risks and progress. Additionally, for major projects, formal project risk assessment would be carried out and managed on an ongoing basis.
8. Components of well-known IT control frameworks will applicable to the LCBF's technology environment may be implemented providing a standardized set of terms and definitions that are commonly interpreted by stakeholders, allowing them to bridge the gap with respect to control requirements, technical issues and business risks, and communicate a level of control.
9. The Company will have and test appropriate Business Continuity Plans as per regulatory requirements.
10. The Company will have an appropriate vendor evaluation process for outsourced services, including comprehensive due diligence procedures, monitoring vendor performance and managing service level agreements.

10 Operational Risk in Outsourcing

10.1 Outsourcing Committee and Outsourcing Policy

The Company had adopted a policy/framework for outsourcing activities in accordance with the Outsourcing Policy of the LCBF as well as Outsourcing guidelines of CBSL. The LCBF shall establish an Outsourcing Committee with the following mandate on Operational Risk issues:

- Evaluate the Operational Risks and materiality of all existing and prospective outsourcing;
- Ensure that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested by the outsourced service providers;
- Review results and follow up of risk assessment of service providers of outsourced activity.
- Discuss Business Continuity Plan reports and Disaster Recovery Plan (DRP) drill outcomes along with Response Time Objectives (RTO). The RTOs would be aligned to the requirement of relevant operations / business groups of the LCBF.
- Undertake periodic reviews (at least annually) of the outsourcing arrangements to identify new material operational and outsourcing risks, if any

- Review Key Performance Indicators of service providers

The Outsourcing Committee to document new outsourcing criteria evaluation, risk assessment, materiality assessment, pre-outsourcing analysis and a cost benefit analysis of the service provider, under Procedural guidelines on outsourcing of the LCBF.

ORM Unit would be involved in conducting operational risk assessments of potential third party outsourced providers at time of on-boarding and on the annual reviews of third party service providers.

10.2 Periodic Review of Performance of the Service Provider

The Outsourcing Committee would decide on the frequency of calls for review of performance of each serviceprovider on the basis of intensity/volume for transactions and the impact of the service in relation to the LCBFs' operations. The parameters that need to be reviewed for operational risk aspects would include TurnAround Times, operational losses, near misses, staff turnover, audit points issued and their compliance, BCP drills schedule and status.

Annual review:

The annual evaluation of service providers will also incorporate their annual performance. This will broadlycover the following areas:

- Extent of operational loss and near miss cases;
- Timeliness and quality of reports submitted;
- External and/or internal audit comments and status of adherence
- Findings and discussions on the basis of physical visits and periodic performance review calls
- Adherence to stipulated SLAs'

11 Risk Register

A risk register is a structured document used in risk management to proactively identify, assess, and manage risks within an organization. It serves as a central repository for tracking risks related to operations, or other business activities.

In the context of finance, a risk register helps finance company anticipate potential obstacles and vulnerabilities, allowing them to take preventive measures.

Risk Register – Main Depository of Key Risks and Controls

- Identified across all department in the company
- Actions to mitigate each risk event

Identified Risks – Result of systematic or Ad hoc Assessments

- Risk control Self – Assessments (RCSA)
- Performed at a given point of time

Risk Register – Essential to Successful Management of Risk

- Plays an important part in Risk Management Plan
- Helps to track issues and address problems

Well Designed and Properly Managed Risk Register

- Offers significant insight into company risk control environment

11.1 Functions of a Risk Register

Central Repository for Identified Risks

- Department – wise risk items with probabilities and impacts
- Action plan and responsibility attached to each risk

Mechanism for Front Line Responsibility

- Operational Risk management and control directly with management

Common Risk Qualification Methodology

- Common sets of values across the Bank

Clear Ownership of Action Plans

- Specific ownership for better accountability

Open Discussion of Risk and Control Matters

- Better transparency and understanding of risk and its implications
- Across the business

12 Risk Heat Map

Identifies impact and likelihood of risk occurrence

- Provides framework for prioritizing risks

Highlights gaps assurances over significant risk areas

- Identifies duplicate or burdensome assurance processes

12.1 Risk Mapping

Potential Loss from Adverse Outcome

- Probability or likelihood of advance outcome
- Impact of outcome if it Assess

Initial Review to identify and assess risks

- Assessment of probabilities and impact based on judgement and experience
- Initial analysis categorizes probability as high, medium, or low

13 Business Continuity Planning

Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to the LCBF and plays a critical role in operational risk management. The plan ensuresthat personnel and assets are protected and are able to function within the stipulated time period without disrupting the activities in the event of a disaster. BCP involves defining any and all risks that can affect the LCBF's operations, making it an important part of the organization's risk management strategy. Risks may include natural disasters—fire, flood, or weather-related events, pandemics, riots, civil commotions to cyber-attacks.

Once the risks are identified, the plan should also include:

- Determining how those risks will affect operations through Business Impact Assessment
- Implementing safeguards and procedures to mitigate the risks
- Testing procedures to ensure they work through BCP and DR drills
- Reviewing the process to make sure that it is up to date

The LCBF has a BCP in place and the ORM Unit would get involved in reviewing and updating BCP and onmonitoring the BCP Test and DR Test results to ensure that there are no material shortcomings on the BCP.

The LCBFs' Business Continuity Plan would detail the risks that are mitigated, procedure and process of BCP.

The BCP Test and DR Test results would be presented to the EIRMC for review and mitigation plans for anyshortcomings that were identified during the tests.

14 New Product / Process Launch, modification and withdrawal

In respect of the process to be followed for launch of new products or modification of the existing products or processes, the Business and/ or Operational Units should seek risk review from the IRMD for Operational Risks, Reputational Risks and Credit and/ or Liquidity, Interest Rate risk (where applicable) prior to submitting for the Product Development Committee approvals and subsequently for Management and Board Level committees. The IRMD is responsible to provide risk reviews including the operational and business controls, risk limits and any mitigations that need to be incorporate.

Subsequent to the launch of the Product or Process, the IRMD is responsible in providing periodic updates to Business Teams, EIRMC and BIRMC on the performance and any improvements that needs at the Product and/ or Process levels. Adherence to Product/ Process guidelines by the first line staff should be done throughthe monthly operational risk check list, process walk through or periodic visits to the Branches. Any deviationsshould be reported back to the Product or Process owners for immediate rectification.

When a Product or a Process is withdrawn, IRMD would be responsible to ensure that there are other Products or Processes which would replace or compliment the withdrawn once to ensure that there are not process gaps, Internal Controls are maintained and Client servicing is not disrupted. Special emphasis shouldbe placed on the transitional arrangements and communications for both internal and external stakeholdersare done accordingly.

15 Insurance Policies

Innovative insurance policies could be used to externalize the risk of 'low frequency and high severity losses',which may occur as a result of events such as errors and omissions, physical loss of securities, frauds and natural disasters.

16 Stress Testing

The finance industry has long been challenged with implementing the concept of operational risk stress testing due to lack of past operational loss data or that there had not been any significant operational loss events. Therefore, stress testing should evaluate the potential vulnerability of the LCBF to exceptional but plausible events that may increase the Operational risk related losses and to ensure that the LCBF has adequate capital to cover such losses.

The hypothetical scenarios that have been considered are:

- People - Inadequacy of quality staff
- Process – Inadequate processes or processes not being followed.
- System- System not functioning as required for a prolonged period of timeExternal – Exposure to robberies and external frauds

The detailed stress testing for operational risk would be discussed in the Stress Testing Policy of the LCBFincluding the scenarios, reporting and escalation process.

17 Capital Allocation

All stakeholders of the LCBF should be conscious of the fact that Capital should be allocated to cover Operational Risk losses. As the complexity and sophistication of the LCBF increases, the importance of maintaining capital buffers becomes paramount.

LCBF would allocate capital for Operational Risk under Capital Adequacy framework as prescribed by CBSL, would follow the **Basic Indicator Approach** as prescribed by the Regulatory Framework.

Annexure – 1 – Key Risk Indicators (KRIs) – Operational Risk

Existing KRIs'

	Risk Indicator	Definition / Description
1	Operational losses not covered by insurance as a % of net income	Charges to P&L on account of operational losses divided by net income
2	Audit Outstanding	Outstanding Issues
3	Customer Complaints	Customer complaints received / resolved
4	Fraud / attempts	Report on detection of frauds/attempts
5	Staff turnover	Maintain staff turnover ratio
6	System down time	Number of system downtime reported whereLCBF operation had any impact
7	Core LCBF System hackings	Number of attempts for hacking the core LCBF system and Number of successful events (if any)
8	Disciplinary Cases	Number of Disciplinary Cases
9	Grievances Cases	Number of Grievances Cases

Common Key Risk Indicators

Type of Common Risk	Risk Indicator
1. Organizational Controls	
Delegated authorities must be assigned and appliedin accordance with policy.	Number of breaches of delegated authority without appropriate approval during the month (Exceeding financial powers, document requirement waivers, etc.)
2. Legal and Compliance	
Staff breaches of Code of Conduct, including ethical standards, integrity, honesty and confidentiality must be reported and investigated in accordance with LCBF guidelines.	Number of incidents of frauds involved duringthe month.

3. Staffing and Human Resources	
Staffing levels must be adequate to meet work loads without imposing undue Operational Risk	% of staff resignations (Cumulative for the year i.e., starting April to date of reporting, to be calculated as - {Number of resignations during the year} / {total number of staff in the department as at the end of reporting period})*100
	Number of approved open positions for the past 2 months.
4. Contingency Planning	
All units must have in place a full set of Contingency Plans comprising Crisis Management, Business Continuity and Disaster Recovery	Number of BCP / DR tests not carried out as per testing calendar in the last 1 year
	Number of instances of business disruption during the month (System down abnormally, natural disasters, strike, terrorist attack etc.)
5. Security and Protection	
Staff, property and information must be adequately protected against internal / external threats	Number of instances where breaches of security rules occur during the month (Examples: instance of thefts, losses, physical damage to property, etc.)
6. Technology	
IT Security policies and standards must be adhered to at all times	Number of Information security breaches during the month (Password sharing, data leakage, Deficiencies in physical IT security. Backup tapes kept in the server room itself, physical access control breaches like un-authorized access to server room etc.)
7. Audit Issues	
There must be agreed action plans, with appropriate deadlines, in place to address all significant control issues identified by Internal Audit.	Number of overdue High and Medium audit issues as at the end of the month

Key Risk Indicators - Information Security

1.	IT Change and Project delivery	Risk emanating from failure of change management that may compromise integrity, availability or confidentiality of IT assets.	Emergency changes
			Changes due to “Errors in Software”
2.	IT Security Management	Risk emanating from external information security attacks	Security breaches or security incidents (includes missing devices) not contained
		Risk emanating from virus/malicious code/Malware attacks not quarantined	Instances of Malicious code and Malware not quarantined on servers
		Financial and reputation risk emanating from external phishing,skimming and other criminal activities.	Number of phishing attacks Time taken to bring phishing site down
		Customer data confidentiality, Customer education	Reports on penetration testing
3.	IT Service delivery	Risk emanating from non - resolution of IT issues in time	Number of incidents/issues (Software/Application issues/ bugs)
		Risk emanating from non-resolution of incidents by IT Help desk	Number of instances of delay and its financial impact

Other Key Important Arears of Operation Risk Mgt

- Incident Reporting Process
- Operation Delegation Authority
- New Product Development Process
- Skill Gap – Transaction Monitoring
- Operation Structure
- Monitoring Mechanism
- Follow up Mitigation System
- Policy Implementation (Procedure / Process)
- Policy Implement Check List
- Key Areas – Internal Audit Analysis

Annexure II - Operation Units

Branches

1. Agunakolapalessa Branch
2. Akuressa Branch
3. Deiyandara Branch
4. Embilipitiya Branch
5. Galle Branch
6. Gampaha Branch
7. Karandeniya Branch
8. Karapitiya Branch
9. Kegalle Branch
10. Kohuwala Branch
11. Kuliyapiya Branch
12. Maharagama Branch
13. Matara Branch
14. Minuwangoda Branch
15. Negambo Branch
16. Pelawatta Branch
17. Rathgama Branch
18. Tangalle Branch
19. Thissamaharama Branch
20. Walasmulla Branch

Head Office Departments

1. Finance & Treasury Department
2. Credit Department (Loan & Leasing)
3. IT Department
4. Administration & Operations Department
5. Legal Department
6. Human Resource Department
7. Recovery Department
8. Business Development and Marketing department
9. Compliance Department
10. Risk Department

Annexure 111 - EIRMC Composition

1. Executive Director/CEO
2. Chief Risk Officer
3. AGM – Finance & Planning
4. DGM– Res. & Mobi.
5. DGM – IT
6. DGM – Credit
7. Head of Compliance

8. Head of Recovery
9. Head of Legal
10. Head of Leasing
11. Head of Gold Loan
12. Head of Business Operation
13. Head of Branch Operations
14. Head of Administration
15. Head of Audit

Annexture IV - ALCO Committee Composition

1. Executive Director/CEO
2. AGM – Finance & Planning
3. Head of Finance
4. Chief Risk Officer
5. DGM– Res. & Mobi.
6. DGM – Credit
7. Head of Compliance
8. Head of Leasing
9. Head of Gold Loan
10. Head of Business Operation
11. Head of Branch Operations
12. Any other by Invitation

Annexture V – Risk Register

Risk ID	Risk Description	Risk Category	Likelihood	Impact	Risk Score	Mitigation Strategy	Risk Owner	Status	Review Date
1	Cybersecurity Threats	Technology	High	High	9	Implement firewalls	IT Manager	In Progress	2024-07-01
2	Regulatory Changes	Compliance	Medium	High	6	Regular audits	Compliance	Open	2024-08-15
3	Employee Fraud	Operational	Low	High	3	Conduct background checks	HR Manager	Closed	2024-09-30
4	Data Breach	Technology	High	High	9	Encrypt sensitive data	IT Manager	In Progress	2024-07-01

5	System Downtime	Technology	Medium	Medium	4	Maintain backup systems	IT Manager	Open	2024-08-15
6	Market Fluctuations	Financial	High	Medium	6	Diversify investments	CFO	Open	2024-09-30
7	Supplier Failure	Operational	Low	Medium	2	Multiple suppliers	Procurement	Closed	2024-07-01
8	Natural Disasters	Environmental	Medium	High	6	Develop a DR plan	Facilities	Open	2024-08-15
9	Customer Complaints	Reputational	Medium	Medium	4	Improve service quality	Customer Service	In Progress	2024-09-30

Incident Type	Description	Likelihood (Low, Medium, High)	Impact (Financial, Operational, Reputational)	Control Measures	Owner	Date Created/Last Updated
Hardware Failure	Failure of critical IT hardware (e.g., servers, storage devices)	[Likelihood Rating]	[Financial Impact, Operational Impact, Reputational Impact]	- Regular hardware maintenance	- IT Infrastructure Team	[Date]
Software Bug	Software malfunction leading to inaccurate data or system disruptions	[Likelihood Rating]	[Financial Impact, Operational Impact, Reputational Impact]	- Implement robust testing procedures	- IT Development Team	[Date]
Cybersecurity Attack	Unauthorized access to IT systems or data (e.g., hacking, phishing)	[Likelihood Rating]	[Financial Impact, Operational Impact, Reputational Impact]	- Implement robust security measures (firewalls, intrusion detection) - Employee cybersecurity awareness training	- IT Security Team	[Date]

System Outage	Unplanned downtime of critical systems (e.g., online banking, payment processing)	[Likelihood Rating]	[Financial Impact, Operational Impact, Reputational Impact]	- Implement high availability architecture and redundant systems	- IT Operations Team	[Date]
Data Loss	Accidental deletion or unavailability of critical data	[Likelihood Rating]	[Financial Impact, Operational Impact, Reputational Impact]	- Regular data backups	- IT Operations Team	[Date]
Power Outage	Loss of power supply impacting IT infrastructure	[Likelihood Rating]	[Financial Impact, Operational Impact, Reputational Impact]	- Implement backup power solutions (UPS, generators)	- Facilities Management Team	[Date]

Annexture VI – Incident Reporting Framework

Incident ID	**Date of Incident**	**Reported By**	**Department**	**Incident Description**	**Impact**	**Severity Level**	**Root Cause**	**Action Taken**	**Status**	**Comments**
INC 001	6/25/2024	Mr. MJ HP	Finance	System downtime	High	Critical	Software bug	Reboot system	Resolved	N/A
INC 002	6/26/2024	Mr. LCB	IT	Unauthorized access	Medium	High	Phishing attack	Changed passwords	Ongoing	Monitoring

Column Descriptions

- Incident ID: Unique identifier for each incident.
- Date of Incident: The date when the incident occurred.
- Reported By: Name of the person who reported the incident.
- Department: The department where the incident was reported.

- Incident Description: A brief description of the incident.
- Impact: The impact of the incident on the business (e.g., High, Medium, Low).
- Severity Level: The severity of the incident (e.g., Critical, High, Medium, Low).
- Root Cause: The identified root cause of the incident.
- Action Taken: Actions taken to address the incident.
- Status: Current status of the incident (e.g., Resolved, Ongoing).
- Comments: Any additional comments or notes regarding the incident.

RECOMMENDATION

……………………..

Chief Risk Officer

………………………………….

CEO/Chief Executive Officer