LCB Finance PLC

GENERAL CIRCULAR No 2024/ 12
15th July 2024

IMPLEMENTATION OF OPERATIONAL RISK MANAGEMENT PROCEDURES AT LCB FINANCE PLC

We have obtained the approval of the Board of Directors to adopt the captioned, Manual to meet the regulatory requirements

1. Introduction

Operational Risk is intrinsic to financial institutions and it should be an important content of an organization-wide Risk Management framework.

We need to control occurrence of potentially damaging Operational Risk events Then Operational Risk Management is structured in compliance with the regulatory requirements,

The goal is to identify, assess, monitor different types of Operational Risks including Information Technology (IT) Risk and establishing controls to mitigate the losses that may arise 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.

The reporting of identified operational risk to the Board of Directors will be through Board Integrated Risk Management Committee (BIRMC) by Chief Risk Officer

All employees are required to read, understand, and comply with the requirements that have been set out herein under the guidance of Business / Operations Heads.

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 the following

a) **<u>Internal Process Risk</u> – 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.**
b) **<u>People Risk</u> – 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.

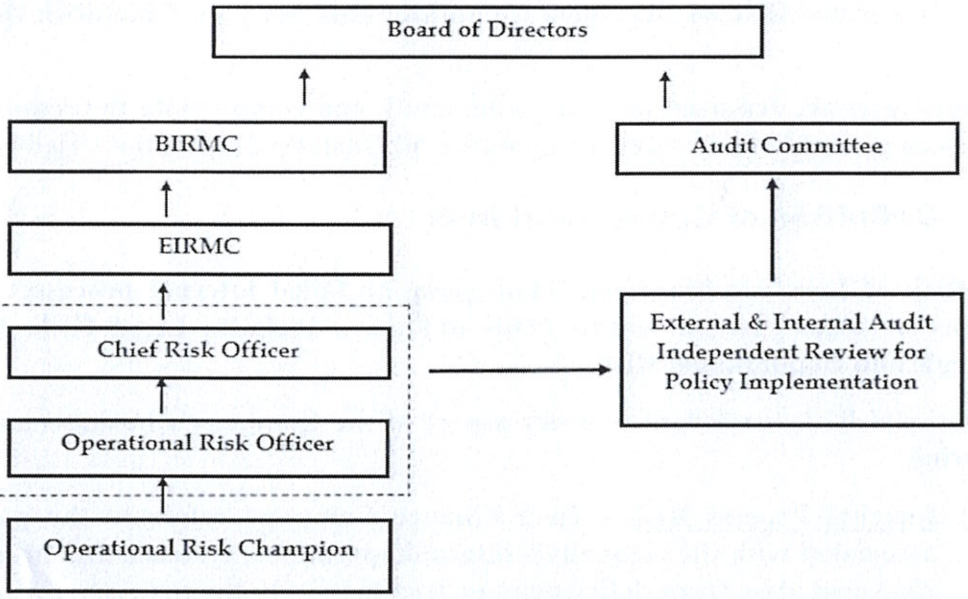
c) **System Risk - In a Finance Company refers to the potential risks associated with the company's information technology (IT) systems and infrastructure. These risks stem from vulnerabilities, failures, or disruption in the company's IT systems, which can have significant consequences for the company's operations, financial stability and reputation.**

Types of Technology Risk

a) **Access Risk – Information may be divulged to unauthorized recipients**
b) **Availability Risk – Service may be lost or data may not be accessible**
c) **Cyber and Information Risk – Failure to safeguard privacy, confidentiality, integrity, and availability of information**
d) **Emerging Technology Risk – Threats associated with new technology**
e) **Infrastructure Risk – IT infrastructure may be unable to support business needs**
f) **Integrity Risk**
g) **Investment or Expense Risk**
h) **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.**

3. 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


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

Key functions and Roles of Operational Risk Champion

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

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

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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.

h) 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.

i) Training and Development: Provide training and guidance to staff members on operational risk management principles, practices, and tools. Promote awareness of risk management best practices and encourage staff involvement in risk identification and mitigation efforts.

j) 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.

4. Incident Reporting system

How it operates:

a) 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 potential risks to the incident reporting system.

b) 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.

c) 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.

d) 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.

e) Every employee within the LCBF has a responsibility to report any incidents or risks they observethrough the incident reporting system.

f) 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.

g) 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.

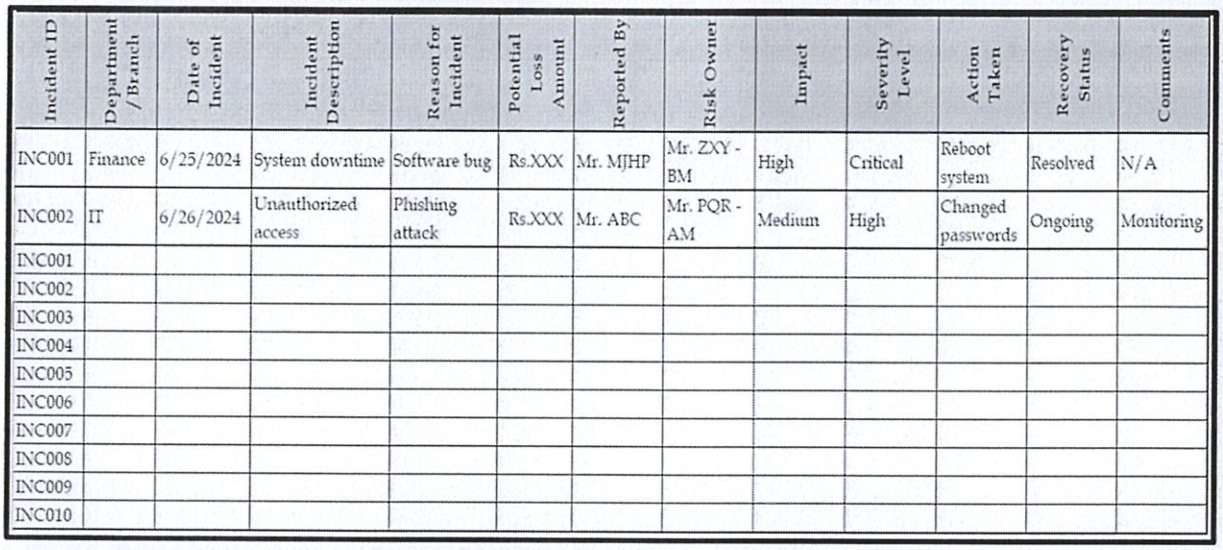
h) Employees are encouraged to report incidents without delay, following established protocols andprocedures outlined in the incident reporting system.

i) The incident reporting system should guarantee confidentiality and protection against retaliationfor employees who report incidents in good faith.

j) Employees should feel safe and supported when reporting incidents, knowing that their concerns will be taken seriously and addressed appropriately by the organization.

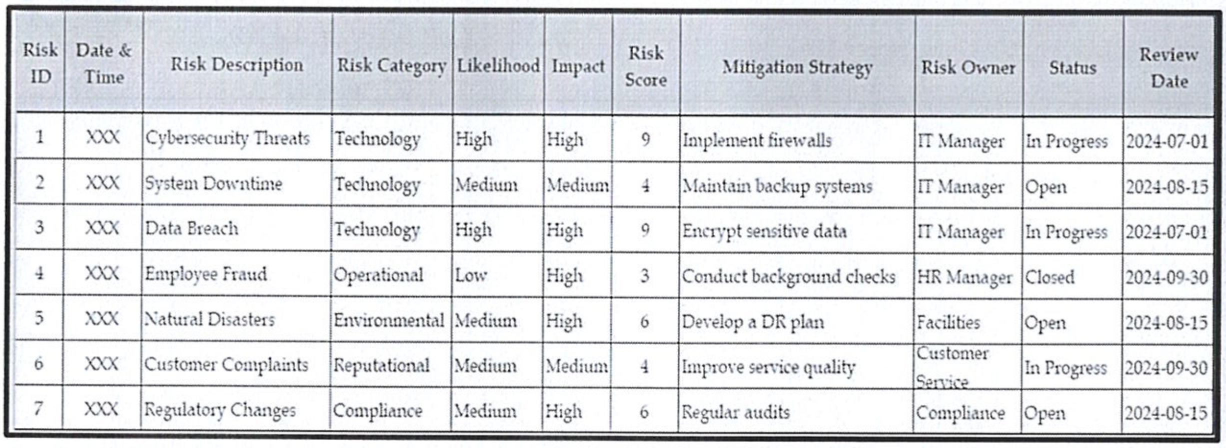
k) The incident reporting system should also facilitate continuous improvement by capturing data onreported incidents. This data can be analyzed to identify trends, recurring issues, or areas of concern, allowing the organization to implement preventive measures and enhance its risk management practices over time.

5. **Sample Data Entry for Incident Reporting Register (EXCEL work sheet will be provided by the Risk Control Department to maintain records untill online reporting system is introduced)**



Incident ID	Department /Branch	Date of Incident	Incident Description	Reason for Incident	Potential Loss Amount	Reported By	Risk Owner	Impact	Severity Level	Action Taken	Recovery Status	Comments
INC001	Finance	6/25/2024	System downtime	Software bug	Rs.XXX	Mr. MJHP	Mr. ZXY - BM	High	Critical	Reboot system	Resolved	N/A
INC002	IT	6/26/2024	Unauthorized access	Phishing attack	Rs.XXX	Mr. ABC	Mr. PQR - AM	Medium	High	Changed passwords	Ongoing	Monitoring
INC001												
INC002												
INC003												
INC004												
INC005												
INC006												
INC007												
INC008												
INC009												
INC010												

Sample Data Entry for Operational Risk Register (EXCEL work sheet will be provided by the Risk Control Department to maintain records untill online reporting system is introduced)



Risk ID	Date & Time	Risk Description	Risk Category	Likelihood	Impact	Risk Score	Mitigation Strategy	Risk Owner	Status	Review Date
1	XXX	Cybersecurity Threats	Technology	High	High	9	Implement firewalls	IT Manager	In Progress	2024-07-01
2	XXX	System Downtime	Technology	Medium	Medium	4	Maintain backup systems	IT Manager	Open	2024-08-15
3	XXX	Data Breach	Technology	High	High	9	Encrypt sensitive data	IT Manager	In Progress	2024-07-01
4	XXX	Employee Fraud	Operational	Low	High	3	Conduct background checks	HR Manager	Closed	2024-09-30
5	XXX	Natural Disasters	Environmental	Medium	High	6	Develop a DR plan	Facilities	Open	2024-08-15
6	XXX	Customer Complaints	Reputational	Medium	Medium	4	Improve service quality	Customer Service	In Progress	2024-09-30
7	XXX	Regulatory Changes	Compliance	Medium	High	6	Regular audits	Compliance	Open	2024-08-15

Completed data sheets from every department/branch should be sent via risk@lcbfinance.net on or before 5th of every month – recorded data regarding prior month.

(Ex: Month of August data sheet – should be sent on or before 5th September)

For any clarifications, please contact Risk Control Department

Mr. Jayalal Hemasiri Perera – Ex No. 205 – Email : jayalal@lcbfinance.lk

Ms. Rangika Vidurangi - Ex No. 232 – Email : rangika.v@lcbfiance.net

Please ensure compliance with immediate effect

15.07.2024

CRO/Chief Risk Officer

CEO/ / Executive Director

5. Sample Data Entry for Incident Reporting Register (NB the work sheet will be provided by the Risk Control Department to maintain consistency within reporting system is maintained)