



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

OPERATIONAL RISK MANAGEMENT

- 1. Legal provisions**

In terms of the powers conferred by Section 12(1) of the Finance Business Act, No.42 of 2011 read with Section 133(1) of the Central Bank of Sri Lanka Act, No.16 of 2023, the Central Bank of Sri Lanka hereby issues these directions on Operational Risk Management to all Finance Companies (FCs) licensed under the Finance Business Act, No.42 of 2011.
- 2. Objectives of the directions**

Establishing a sound operational risk management framework through formulation of operational risk management policy and procedures, operational risk governance structure and effective operational risk management processes across the FC to identify, assess, monitor and report, and control and mitigate operational risk while ensuring delivery of uninterrupted services to the customers.
- 3. Applicability**
 - 3.1 These directions outline the key principles for a sound operational risk management framework and the FC shall adopt the principles and practices provided in these directions.
 - 3.2 The FCs with assets of Rs.100 billion and above shall comply with these directions with effect from 01.01.2026, and FCs with assets less than Rs.100 billion shall comply with these directions with effect from 01.01.2027.
- 4. Operational risk management framework**
 - 4.1 The operational risk management framework shall aim to provide a structured and systematic approach to ensure effective management of operational risk by the FC, to minimize the operational risk losses resulting from inadequate or failed internal processes, people and systems, or from external events.
 - 4.2 The operational risk management framework shall ensure that FC maintains operational resilience i.e. the ability to deliver critical operations during disruption/s. Maintaining operational



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

resilience involves a comprehensive and practical approach to identify, prepare for, respond to and recover from disruptive events, in order to minimize their impact on the continuity of critical business operations.

4.3 The operational risk management framework shall be in line with the FC's risk profile, its risk appetite and capital management strategies, taking into account of internal and external risk factors and covering all business lines and functions of the FC.

4.4 The operational risk management framework of the FC shall at least contain the following elements:

- a) Operational risk management policy and procedures;
- b) Operational risk governance structure; and
- c) Operational risk management process.

4.5 **Operational risk management policy and procedures**

- a) The FC shall have policy and procedures outlining the primary elements of the operational risk management framework including identification, assessment, monitoring, controlling, reporting, mitigating and public disclosure.
- b) The operational risk management policy and procedures shall be documented, consistent with the best practices and reviewed at least annually.
- c) At a minimum, the operational risk management policy and procedures shall outline the following:
 - i. Provide a common operational risk taxonomy including the definition of operational risk and operational losses to ensure consistency of risk identification and exposure rating;
 - ii. Description of the FC's accepted operational risk appetite, tolerance level and limit for residual risk;



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

- iii. Identification of governance structure used to manage operational risk, including reporting lines and accountabilities;
- iv. Description of the risk assessment tools i.e. self - assessments, operational risk event dataset, key risk indicators, scenario analysis, etc.;
- v. Description of risk controls, mitigation strategies and instruments;
- vi. Independent review and assessment of operational risk; and
- vii. Risk reporting.

4.6 Operational risk governance structure

- a) The FC shall have a sound governance structure to support successful formulation and implementation of an effective operational risk management framework.
- b) Board of Directors (BoDs) / Board Integrated Risk Management Committee (BIRMC) is primarily responsible for ensuring effective management of operational risk.
- c) The responsibilities of the BoDs / BIRMC shall include at a minimum:
 - i. Establishment of a strong operational risk management culture to understand the nature and the scope of the operational risk and a control environment that are fully integrated into or coordinated with the overall risk management framework of the FC;
 - ii. Approving and reviewing operational risk management policy and procedures to ensure that the risks arising from the changes in internal factors such as FC's structure, the nature of the activities, the



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

-
- quality of personnel, systems and controls, and external factors such as broader environment and the industry and advancement in technology are taken into consideration;
- iii. Providing senior management with clear guidance and direction regarding the principles underlying the operational risk management framework;
 - iv. Overseeing material operational risks and effectiveness of control environment to ensure that senior management implements the operational risk management policy, procedures and systems effectively at all levels; and
 - v. Ensuring that FC's operational risk management framework is subject to independent review by internal audit.
- d) Senior Management of FC / Senior Management-Level Committee shall:
- i. Develop clear and sound operational risk management policy and procedures for the approval of BoDs / BIRMC and implement them effectively;
 - ii. Assign authority, responsibility and reporting lines to encourage and maintain accountability and ensure that the necessary resources are available to manage operational risk in line with the FC's risk appetite and tolerance levels;
 - iii. Ensure that the operational risk management policy has been clearly communicated to relevant staff at all levels;
 - iv. Develop and implement adequate internal controls to mitigate the operational risk; and



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

- v. Develop appropriate Management Information Systems (MIS) and submit operational risk report to the BoDs / BIRMC.
- e) The FC shall have three lines of defense mechanism in order to facilitate a sound operational risk management process.
 - i. The heads of business units and / or branch managers shall be responsible for identifying and managing the risks inherent in the products, activities, processes, and systems that they own.
 - ii. The Chief Risk Officer shall be responsible for monitoring the effective implementation of risk management framework, facilitate high levels of risk awareness throughout the FC and carry out measurement, monitoring and reporting to BoDs / BIRMC.
 - iii. The Chief Internal Auditor shall be responsible for performing an independent review on effectiveness of the operational risk management framework, including policy and procedures and compliance with the policy and procedures.

4.7 Operational risk management process

The FC shall have an effective operational risk management process which shall formalize the FC's approach to the following:

a) Identification and assessment

- i. The FC shall have in place comprehensive processes for identification and assessment of operational risks inherent in all products, activities, processes, and systems. Effective risk identification considers both internal and external factors.
- ii. At a minimum, the FC shall use the following tools for



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

identifying and assessing the operational risk of the company. Guidelines for developing such tools are set out in Annexure A.

- a. Self-risk assessment
- b. Operational risk event dataset
- c. Key risk indicators
- d. Scenario analysis

b) Monitoring and reporting

- i. The FC shall implement a process to regularly monitor operational risk profile and material risk exposure.
- ii. The FC shall have appropriate reporting mechanisms including incident reporting in place at all levels such as BoDs / BIRMC, senior management and business units that support proactive management of operational risk. An operational risk report shall be submitted to the BoDs / BIRMC at least quarterly and whenever there is a significant change in the operational risk profile of the FC. The operational risk report should include the following.
 - a. Risk exposures of the FC;
 - b. Breaches of FC's risk appetite, tolerance level and limits, if any;
 - c. Details of recent significant operational risk events and losses, if any;
 - d. Brief elaboration and assessment of key and emerging risks;
 - e. Mitigation strategies; and
 - f. Relevant external events or regulatory



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

changes and any potential impact on the FC.

- iii. The FC shall ensure that data capturing, and risk reporting processes are reviewed at least annually with a view to continuously enhancing risk management as well as to improve risk management policy and procedures.

c) Control and mitigation

- i. The FC shall have a strong control environment that utilizes policy, processes and systems, appropriate internal controls, and appropriate risk mitigation strategies to deliver uninterrupted services to the customers.
- ii. The FC shall ensure that there are appropriate segregation of duties and personnel are not assigned with conflicting responsibilities. Areas of potential conflicts of interest shall be identified, minimized, and be subjected to careful independent monitoring and review.
- iii. The FC shall ensure that other common internal controls are in place as appropriate to address operational risk such as well-established authority levels and approval processes, risk limits, physical and virtual access controls and verifications and reconciliations, etc.
- iv. The FC shall aim to effectively utilize technologies to automate the business processes as a control measure.
- v. The FC shall have a business continuity and disaster recovery plan in place as a part of the operational risk management framework to ensure



**GOVERNING BOARD
CENTRAL BANK OF SRI LANKA**

29 November 2024

FINANCE BUSINESS ACT DIRECTIONS

No.04 of 2024

its ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.

- vi. The FC can complement controls by seeking to transfer risk to another party such as through insurance. However, risk transfer cannot be a substitute for sound controls and risk management programs.

5. Public disclosure

The FC shall provide key elements of its operational risk management framework and relevant information to stakeholders depending on the size, risk profile, complexity of FC's operations, and evolving industry practice, enabling them to assess operational risk exposure of the FC and the approach to operational risk management, under the management report in the annual report of the FC or website of such FC.

6. Reporting of loss events

FCs shall report details of operational loss events to the Director, Department of Supervision of Non-Bank Financial Institutions (DSNBFI) on a periodic basis enabling DSNBFI to proactively assess the emerging operational risk in the sector. The reporting format will be specified by DSNBFI under Financial Information Network Reporting System (FinNet).

Dr. P Nandalal Weerasinghe
*Chairperson of the Governing Board and
Governor of the Central Bank of Sri Lanka*

Guidelines on Developing Tools for Identifying and Assessing Operational Risks of FCs

1. Self-risk assessment

- i. The FC shall perform self-risk assessments of its operational risks and controls on different levels. The assessments typically evaluate inherent risks (the risks before controls are considered), the effectiveness of internal controls, and residual risks (the risk exposures after controls are considered) and contain both quantitative and qualitative elements.
- ii. The FC shall perform self-risk assessments across all areas and activities (such as information technology, treasury, customer services, payments, financial controls, business development, etc.) within the business that has the potential to pose an operational risk to the FC.
- iii. Following identification, the FC shall assess, existing controls that have already been created or assigned to mitigate the identified risk and the FC shall prioritize the identified risks on the basis of high, medium, or low – while inherent risks and residual risks are segregated.
- iv. A risk register shall be maintained to collate this information to form a meaningful view of the overall effectiveness of controls and facilitate oversight by senior management, and the BoDs.
- v. The FC may use the self-risk assessment to improve the internal controls of the FC by increasing awareness regarding FC’s objectives and facilitate effective design and implementation of control processes.

2. Operational risk event dataset

- i. The FC shall maintain a comprehensive operational risk event dataset that records all material events experienced by the FC/ industry which serves as a basis for operational risk assessments.
- ii. The operational risk event dataset may typically include internal loss data, near misses, and, when feasible, external operational loss event data (external data are indicators of risks that are common across the industry).

3. Key Risk Indicators

- i. Key Risk Indicators (KRI) are statistics and/or metrics, which can provide insight into the FC's risk exposure. These indicators shall be reviewed on a periodic basis (such as monthly or quarterly) to alert the FC on changes that may be indicative of risk concerns.
- ii. When developing KRI, the FC shall consider the areas and functions, potential risks, and threats and vulnerabilities it faces.
- iii. KRIs are developed in relation to the FC's processes, people, systems and external events capturing at a minimum following loss event types specified in Table 1, below. KRIs also provide measurement points that, if exceeded, could disrupt the business.

Table 1: Loss event types and examples

Event type	Explanation	Examples
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy excluding diversity/discrimination events, which involves at least one internal party.	Employee theft, intentional misreporting of positions, and insider trading on an employee's own account
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	Theft/robbery, forgery and cheque fraud
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims or from diversity/discrimination events.	Workers' compensation and discrimination claims, violation of employee health and safety rules and general liability
Products and business practices	Losses arising from an unintentional, negligence or failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Misuse of confidential customer information, money laundering and carrying out of unauthorized business
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Terrorism, earthquakes, fire and floods
Business disruption and system failures	Losses arising from disruption of business or system failures.	Hardware and software failures, telecommunications problems, and utility outages
Execution, delivery and process management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	Data entry errors, collateral management failure and incomplete legal documentation

4. Scenario analysis

- i. Scenario analysis is a process to identify possible high-impact events and shall be considered in forward looking operational risk analysis.
- ii. The FC may brainstorm all possible scenarios that could lead to negative outcomes in business areas and functions. These include internal risks such as fraud, sabotage, data breaches etc., as well as external risks such as natural disasters or economic downturns.
- iii. Once the FC has identified potential scenarios, the FC should evaluate the probability of occurrence of each such scenario and its potential impact on the business.
- iv. The FC should develop strategies for each scenario based on above assessment. These strategies shall support prevention or mitigation of any negative impact on FCs business operations.