Commercial Credit & Finance PLC

Operational Risk Management Policy

Contents

1. Purpose

This policy establishes a structured framework for managing operational risks that may impact the financial, reputational, legal, or regulatory standing of Commercial Credit & Finance PLC. The goal is to minimize the frequency and impact of risk events that may arise from inadequate or failed internal processes, people, systems, or external events. Purpose of this framework is identification, assessment, monitoring, controlling, reporting, mitigating and public disclosure of operational risks, ensuring the stability and resilience of business operations. This policy has been developed in accordance with the Finance Business Act Directions No. 04 of 2025 on Operational Risk Management, issued by the Central Bank of Sri Lanka.

2. Version Control

This policy will be reviewed once a year or in the event of any changes in the regulatory, management or environmental requirements. The updates will be recorded in the "Version Control" section.

Version Code	Released Date	Prepared by	Approved by
1.0	31st January 2024	Chief Risk Officer	Board of Directors
2.0	31st October 2025	Chief Risk Officer	Board of Directors

3. Scope

This policy applies to all departments, employees, systems, and third-party service providers engaged by Commercial Credit & Finance PLC.

4. Definitions

- **Operational Risk**: Risk of loss from inadequate or failed internal processes, people, systems, or external events.
- **Risk Appetite**: The level of risk Commercial Credit & Finance PLC is willing to accept in pursuit of its objectives.
- **KRI (Key Risk Indicator)**: A metric used to signal the potential of future operational risk events.

5. Risk Appetite, Tolerance Level and Residual Risk

The Board of Directors will determine the risk appetite, tolerance levels, and residual risk thresholds for key risk areas, considering the company's strategic objectives, industry trends, and regulatory requirements. These limits will be outlined in the Risk Appetite Statement, which will be reviewed on an annual basis by the Board.

6. Operational Risk Governance Structure

Role	Responsibility
Board of Directors	Oversight and approval of ORM policy and risk appetite
Board Integrated Risk Management Committee	Strategic direction and oversight of ORM framework
Senior Management, Business Units and Branches	Identification and first-level management of operational risks

Risk Management and Compliance Departments	Independent monitoring of effective implementation of risk management framework
Internal Audit Department	Providing independent and objective assurance on the risk management processes and practices in place

7. Roles and Responsibilities

- The board of directors should approve the policy for operational risk management.
- The periodic high risk findings of Risk Control Self-Assessment (RCSA) should be evaluated by the BIRMC.
- The senior management is responsible for operationalizing board approved policies and inculcating an organizational culture that places high priority on sound internal controls and procedures.
- The senior management is responsible for oversee the development and testing of business continuity plans (BCP) and disaster recovery plans (DRP).
- The heads of the departments and functions are ultimately accountable for carrying out the RCSA assessment.
- Department heads/business heads are ultimately responsible for assessing the design and the performance of controls.
- All business heads and branch managers are deemed the first-line-of-defense and are held accountable for identifying and managing risk and operating within the approved risk policies.
- The second-line-of defense comprises the Risk Management Team (RMT) and the Compliance Team (CT) headed by independent CRO and CO respectively.
- The RMT monitors all key risks in line with Board approved appetite.

- Internal audit team and external auditors act as the third-line-of-defense in providing independent assurance regarding the overall efficacy of the Company's operational risk management.

8. Operational Risk Management Procedure

The operational risk management procedure includes the following key steps:

8.1 Risk Identification

Objective: Proactively discover sources of operational risk before they lead to loss events.

Key Methods:

- **Risk and Control Self-Assessments (RCSA):** Business units map their key processes, identify associated risks, and evaluate existing controls.
- **Process Mapping:** End-to-end documentation of workflows to highlight vulnerable steps (e.g., manual data entry, approval gaps).
- **Incident Data:** Analysis of historical internal loss events or external data (e.g., frauds in peer institutions).
- **Change Management:** Risk assessments for any new products, services, systems, or third-party relationships.
- **Third-Party Risk Reviews:** Assess operational risk exposure from vendors and service providers.

Deliverable:

- A **comprehensive risk register** capturing risks, processes, owners, and current controls.

8.2 Risk Assessment

Objective: Measure and prioritize operational risks to focus resources on the most critical exposures.

8.2.1 Risk Rating

Use a **Risk Matrix** to assess:

- **Impact** (financial loss, reputational damage, regulatory impact, customer harm)
- **Likelihood** (how often the event might occur)

8.2.2 Risk Scoring Example

Impact	Likelihood				
		Remote	**Possible**	**Likely**	**Certain**
	Low	Low	Low	Medium	Medium
	Medium	Low	Medium	High	High
	High	Medium	High	High	Very high
	Critical	Medium	High	Very high	Very high

8.3 Risk Control

Objective: Design and implement controls to reduce the likelihood or impact of operational risk events.

8.3.1 Types of Controls:

- Preventive: Aim to stop an error or event (e.g., segregation of duties, system access controls)
- Detective: Identify issues post-occurrence (e.g., reconciliations, audit trails)
- Corrective: Limit impact and restore normalcy (e.g., backup systems, incident response plans)

Control Documentation:

Each control must be:

- Owned by a responsible person
- Clearly described (objective, method, frequency)
- Tested regularly

8.4 Risk Monitoring

Objective: Track risk levels and control effectiveness over time using quantitative and qualitative tools.

8.4.1 Monitoring Tools

- **Key Risk Indicators (KRIs):** Metrics that serve as early warning signs (e.g., number of failed transactions, staff turnover in critical roles)
- **Control Self-Assessments:** Periodic reviews by business units
- **Dashboards:** Aggregated view of risk ratings, events, and trends
- **Audit & Assurance Reports:** Highlight control gaps or breakdowns

8.5 Risk Reporting

Objective: Provide timely, accurate, and actionable risk information to decision-makers (The Board of Directors, BIRMC, Senior Management).

8.5.1 Frequency & Audience

- **Integrated Risk Management Committee:** summary of top operational risks, trends, and material incidents, Incident details, control gaps, remediation plans
- **Senior Management:** Monthly dashboards and open issues

9. Public Disclosure on Key Elements of Operational Risk Management Framework

The company must disclose the key components of its operational risk management framework to stakeholders, enabling them to assess the company's operational risk exposure and its approach to

managing these risks. This information should be made available in the annual report or on the company's website.

10. Reporting of Operational Loss Events to DSNBFI

The company shall periodically report details of operational loss events to the Director of the Department of Supervision of Non-Bank Financial Institutions, using the reporting format prescribed under the Financial Information Network Reporting System (FinNet).

End of the Document

Recommended by the BIRMC on 21st October 2025

Approved by the BOD on 31st October 2025