Edel Finance Company Limited

Operational Risk Management Policy

Date of Approval	**November 8, 2022**
Version No.	**1**
Previous versions and dates of approval	**-**

1. Objective:

Operational Risk Management Policy (the Policy) sets out the broad principles by which the operational risk is managed such that the risk taken is within the risk tolerance parameters. The Senior Management and the Leadership Team plays the key role in monitoring and managing the operational risk.

The objective of the Policy is to support the overall governance framework and monitor operational risk related aspects in the Company.

The Policy focuses on:

- Assessing and measuring the magnitude of risks, its monitoring and mitigation techniques
- Identification of risks by registering all potential operational risks according to process, products, systems, and external events
- Risk measurement is performed through periodic tracking of KRI's and through loss events database
- Putting in place a suitable organisation structure.

2. Definition of Operational Risk

Operational Risk is defined as "The risk of loss resulting from inadequate or failed internal processes, system controls or human negligence". The definition includes legal risk but excludes strategic and reputation risk.

The Company has identified the following as key areas of operational risk:

a. People Risk
b. Process Risk including data leakage risk
c. Fraud Risk

3. Operational Risk Implementation approach:

The overall approach of the Operational Risk Management (ORM) Framework will be as under:

- The Policy to monitor and guide the operational risk management for the Company
- Business and support functions are responsible for identifying and mitigating risk arising in their respective department.
- Emphasis on monitoring the operational risk/key risk indicators.
- Setting up of tolerance limits for identified key risk indicators.
- Analysis of reported operational risk events and developing mitigating strategies to avoid their occurrence.
- Finance Team/Chief Risk Officer (CRO) has an oversight on ORM framework and update to be provided to the Group Risk Management Committee (GRMC) as and when required.

4. Organisation structure

The organisation for supporting operational risk management governance will include the following:

- Board of directors
- Group Risk Management Committee (GRMC)
- Finance Team
- CRO.

The Board of Directors ensures effective management of the operational risks in the Company. GRMC reviews and evaluates the overall risks assumed by EFCL. The Finance Team/CRO implements the operational risk management framework approved by the Board.

CFO is responsible for risk taking, related controls and mitigations.

5. Operational Risk Management Process

The Company has adopted operational risk management policy that focuses on:

• Assessing and measuring the magnitude of risks, its monitoring and mitigation techniques

• Identification of risks by registering all potential operational risks according to process, products, systems, and external events.

• Risk measurement is performed through periodic tracking of KRI's.

• Putting in place a suitable organization structure.

Operational risk management process comprises of identification, assessment, measurement, mitigation, monitoring and reporting of operational risk.

i. Risk measurement

It involves assessing impact of the events within operating environment of organisation and taking necessary corrective action as and when required. The Operational losses have financial impact that is recorded in financial statement but will not include opportunity cost and forgone revenue.

ii. Risk Monitoring

The mitigation and control of operational risk is mainly done through ongoing monitoring of the Company's systems of internal controls by various departments of the Company. The broad control operational risk sensitive areas which the Company monitors are:

- Control of outsourcing arrangements
- New product approvals
- Monitoring and control of payments and settlements
- Technology risk and Information Security
- Adherence to KYC and Money Laundering Norms.

The Risk Monitoring would be performed basis below activities:

Key Risk indicators: KRIs establish relevant measures (qualitative and quantitative) which enable regular monitoring of trends with regards to risk exposures. Such indicators may include staff turnover, frequency and severity of errors and omission etc. KRI is key component to support risk monitoring and assessment.

Control Testing: The objective of control testing is to assess the operating effectiveness of controls. The Finance Team/CRO may suggest as a part of internal audit to conduct control testing for certain process as part of their annual review. The gaps, if any, identified during testing are reviewed by business and support functions and remediation plan is finalised.

Management information system: In addition to above the Finance Team/CRO tracks and monitors the overall performance of operational risk through a periodic monitoring of combination of open issues and KRIs to assess the effectiveness of controls.

New to product and process : The organisation should ensure once new products are approved, these are shared with the Finance Team/CRO to identify the operational risks jointly with the concerned units. Similarly, for all new/modified processes which are introduced or undertaken, the operational risk inherent in them needs to be identified. Hence all new/modified process post approval would be shared with the Finance Team/CRO for assessment of business identified

operational risks and proposed risk mitigations.

6. Risk Mitigation:

The risks can be mitigated through one of the following broad areas.

- Mitigate or control the identified risk through reducing severity or frequency of the event.
- Accept the risk as a cost of running the business.
- Transfer the risk through mechanisms like insurance or outsourcing activities.
- Avoid the risk by not undertaking the specific activity.

7. Risk Reporting

A consistent approach is adopted for operational risks reporting by providing pertinent information to senior management which includes the following:

- Exceptions in KRIs above tolerance limit.
- Findings, if any, from process reviews.
- Analysis of incidences, if any, reported by business and functions .

8. Review of Operational Risk management Policy

The Policy shall be reviewed by the Board as and when necessary or at least once in two years.