RISK MANAGEMENT POLICY

GLOSEC FINANCE PRIVATE LIMITED

(Base Layer NBFC)

Introduction

The Board of Directors ("Board") of Glosec Finance Private Limited in its Board meeting held on _____, had adopted this Risk Management Policy, which outlines the framework and practices for identification, assessment, monitoring, and mitigation of risks associated with the Company's core business operations.

Purpose

Operational Risk is inherent in all financial products, services, activities, processes, and systems. For a Reporting Entity effective management of such risks is essential to ensure orderly conduct of business and protection of the Company's assets and operations. The purpose of this Policy is to establish a proportionate and structured risk management framework for the company to identify, assess, monitor, and mitigate risks that may arise in the course of its business activities, including unforeseen or unintended risks, while pursuing its strategic objectives.

This Policy is aligned with the regulatory expectations prescribed by the Reserve Bank of India under:

- Guidance Note on Operational Risk Management and Operational Resilience dated November 28, 2025; and
- Reserve Bank of India (Non-Banking Financial Companies – Scale Based Regulation) Directions, 2025 dated 28th November, 2025.

This Policy also aims to ensure that critical functions, where applicable, continue with minimal disruption, thereby safeguarding the interests of the Company and maintaining overall financial stability.

Objective

The objective of this Policy is to establish a comprehensive, proportionate, and effective risk management framework for Glosec Finance Private Limited and to ensure prudent management of risks across all its business activities.

In furtherance of the above, this Policy aims to:

1. Establish Structured Risk Management Framework

To design and implement a well-defined and systematic framework for risk management that is appropriate to the size, scale, complexity, and nature of the Company's operations as an NBFC-BL, ensuring clear roles, responsibilities, and accountability across all levels of the organisation.

2. Risk Identification, Assessment, and Mitigation

To ensure timely identification, evaluation, monitoring, and mitigation of all material risks, including but not limited to credit risk, liquidity risk, operational risk, and other emerging risks, through appropriate tools, internal controls, and risk management practices.

3. Strengthening Operational Resilience

To maintain adequate preparedness to manage operational disruptions by implementing reasonable and proportionate measures for business continuity, data protection, and incident management, thereby ensuring continuity of critical operations, where applicable.

4. Regulatory Compliance

To ensure ongoing compliance with applicable regulatory requirements, guidelines, and directions issued by the Reserve Bank of India, including the Scale Based Regulation (SBR) framework and the Guidance Note on Operational Risk Management and Operational Resilience, as amended from time to time.

5. Protection of Assets and Interests

To safeguard the Company's financial assets, information systems, human resources, and reputation by establishing robust internal controls and risk mitigation strategies.

6. Promote Risk-Aware Culture and Governance

To foster a culture of risk awareness and accountability across the organisation, supported by effective governance mechanisms, including oversight by the Board of Directors and senior management.

7. Support Sustainable Growth

To enable informed decision-making and responsible risk-taking aligned with the Company's strategic objectives, ensuring long-term sustainability, financial stability, and resilience of the business.

Scope

This Risk Management Policy shall apply across the entire organisation and covers all departments, business functions, and operational units of the company. The Policy extends to all activities, products, services, processes, systems, and resources of the Company that may expose it to risks, including but not limited to operational risk, credit risk, liquidity risk, and other associated risks relevant to its business operations.

The scope of this Policy includes:

- All internal processes, systems, and workflows, including technology and information systems
- All employees, management personnel, and functional heads responsible for carrying out business activities
- All business activities and support functions that contribute to the Company's operations
- All third-party arrangements and outsourced activities, to the extent applicable
- All existing and new products, services, and processes introduced by the Company

Categories Of Risks, Causes & Mitigation Measures

Risk Category	Key Causes	Preventive / Mitigation Measures
Credit Risk	i. Borrower default or delayed repayment ii. Weak credit appraisal iii. Concentration in specific sector/borrower iv. Economic downturn affecting repayment capacity	i. Robust credit appraisal and underwriting standards Defined exposure limits and diversification ii. Credit scoring and due diligence iii. Continuous monitoring and early warning systems
Liquidity Risk	i. Asset-liability mismatch ii. Delayed receivables iii. Over-dependence on short term funding iv. Unexpected cash outflows	i. Maintain adequate liquidity buffers ii. Cash flow forecasting and ALM monitoring iii. Diversified funding sources iv. Contingency funding plan
Operational Risk	i. Process failures or weak internal controls ii. Human errors or fraud iii. System failures or cyber incidents iv. Poor documentation or compliance gaps	i. Strong internal controls and SOPs ii. Segregation of duties iii. Staff training and awareness iv. IT security and data backup systems v. Regular internal audits
Compliance / Regulatory Risk	i. Non-compliance with RBI guidelines ii. Inadequate regulatory tracking iii. Weak internal compliance framework	i. Regular compliance monitoring ii. Appointment of compliance function iii. Periodic regulatory updates and training iv. Internal compliance audits
Market Risk	i. Interest rate fluctuations Changes in market conditions ii. Valuation changes in investments	i. Conservative investment strategy ii. Monitoring of interest rate exposure iii. Periodic review of portfolio
Reputational Risk	i. Poor customer service ii. Regulatory non-compliance iii. Negative publicity or fraud incidents	i. Strong ethical practices and governance ii. Transparent communication iii. Prompt grievance redressal iv. Crisis management framework

Legal Risk	i. Defective documentation ii. Contractual disputes iii. Non-compliance with laws	i. Proper legal vetting of documents ii. Standardized agreements iii. Periodic legal review and compliance checks
Strategic Risk	i. Poor business decisions ii. Inadequate planning iii. Changes in market environment	i. Board oversight and strategic planning ii. Periodic business review iii. Risk-aligned decision making
Fraud Risk	i. Internal/external fraud ii. Weak controls or oversight iii. Lack of employee screening	i. Anti-fraud policies and controls ii. Employee background checks iii. Whistle-blower mechanism iv. Regular audits and monitoring

Risk Governance Structure

The Risk Governance Structure of establishes a framework for effective oversight, accountability, and management of risks, ensuring alignment with the Company's strategic objectives and defined risk appetite. The company has adopted three-lines-of-defence model namely:

I. First Line of Defence – Business Units / Functional Heads

The first line of defence comprises Business Unit Heads and Departmental Heads, who are primarily responsible for managing risks inherent in their respective functions, activities, and processes.

In discharging their responsibilities, they shall:

- Identify and assess material risks, including operational risks, using appropriate risk management tools
- Establish, implement, and maintain effective internal controls to mitigate identified risks
- Periodically evaluate the adequacy and effectiveness of such controls
- Report any gaps in resources, systems, or training that may impact risk management
- Monitor and report risk exposures and ensure adherence to the Company's defined risk appetite and tolerance levels
- Report residual risks, including operational loss events, control weaknesses, process deficiencies, and instances of non-compliance

This approach ensures that risk management is embedded within day-to-day operations and promotes accountability at the functional level.

I. Second Line of Defence – Risk Management & Compliance Function

The second line of defence comprises the Risk Management and Compliance functions. In a Base Layer NBFC, these functions may be **combined or operate with limited resources**, while maintaining appropriate independence through segregation of duties.

This function is responsible for oversight of risk management and shall:

- Provide an independent assessment of key risks and effectiveness of controls
- Review and challenge risk identification, measurement, and reporting by business units
- Develop and maintain risk management policies, procedures, and frameworks
- Monitor the overall risk profile of the Company and report to Senior Management and the Board
- Ensure compliance with applicable regulatory requirements issued by the Reserve Bank of India
- Promote risk awareness through training and guidance across the organisation

This function ensures that risks are managed in a consistent and controlled manner across the Company.

III. Third Line of Defence – Internal Audit

The Internal Audit function serves as the third line of defence and provides **independent assurance** to the Board regarding the adequacy and effectiveness of the Risk Management Framework.

The function shall remain independent of the first and second lines of defence and may be performed by internal auditors, external professionals, or qualified third parties.

Its scope includes:

- Reviewing the design and effectiveness of the risk management framework and internal controls
- Verifying the implementation of policies, procedures, and governance processes
- Assessing the reliability and integrity of risk data, assumptions, and methodologies
- Evaluating compliance with applicable laws, regulations, and internal policies
- Identifying gaps, weaknesses, and control deficiencies and reporting them to the Board
- Ensuring timely and appropriate corrective actions are taken by management
- Providing an independent opinion on the overall adequacy and effectiveness of the risk management framework

Risk Management Procedure

The Company shall adopt a systematic and continuous process for managing risks across its operations. The Risk Management Procedure is designed to ensure timely identification,

assessment, mitigation, monitoring, and reporting of risks, thereby supporting effective decision-making and operational stability.

The key steps involved in the Risk Management Procedure are as follows:

1. Risk Identification

The Company shall identify all potential internal and external risks that may impact its operations, financial position, or reputation.

- Business and functional heads shall be responsible for identifying risks within their respective areas
- Risks may arise from processes, systems, people, external events, or regulatory changes
- Both existing and emerging risks shall be periodically identified and documented

2. Risk Assessment

Identified risks shall be evaluated to determine their significance and potential impact.

- Risks shall be assessed based on **likelihood and impact**
- Classification into **high, medium, or low risk categories**
- Maintenance of a **Risk Register** capturing key risks, causes, and controls
- Consideration of both inherent risk and residual risk after applying controls

3. Risk Mitigation and Control

Appropriate measures shall be implemented to manage and mitigate identified risks.

- Implementation of internal controls, policies, and standard operating procedures
- Segregation of duties and defined authorization levels
- Adoption of preventive and detective controls
- Use of technology and system-based controls, wherever feasible
- Risk treatment strategies may include avoidance, reduction, sharing, or acceptance

4. Monitoring and Reporting

The Company shall continuously monitor its risk exposure and control effectiveness.

- Use of **Key Risk Indicators (KRIs)** and periodic risk reviews
- Regular reporting of risk status to Senior Management and the Board
- Escalation of significant risks, breaches, or control failures
- Tracking of risk mitigation actions and timelines

5. Testing and Review

The effectiveness of risk management practices shall be periodically evaluated.

- Internal audits and independent reviews shall be conducted
- Stress testing or scenario analysis may be carried out, where relevant
- Identification of control gaps and implementation of corrective actions

6. Policy Review and Continuous Improvement

The risk management framework shall be reviewed on an ongoing basis.

- Policies and procedures shall be updated based on:
  - Changes in business environment
  - Regulatory updates
  - Internal audit findings and risk events
- Lessons learned from past incidents shall be incorporated to strengthen controls

7. Documentation and Record Keeping

- All risk management activities, assessments, and reports shall be properly documented
- Risk registers, audit reports, and compliance records shall be maintained for reference and regulatory purposes

Risk Management Committee

The Company may constitute a Risk Management Committee ("RMC") to assist the Board of Directors in overseeing the implementation of the Risk Management Policy and monitoring the Company's risk profile.

The Committee shall review key risks, adequacy of internal controls, and effectiveness of risk mitigation measures, and report its observations to the Board periodically. Risk Management Committee shall identify the various type of risks involved in the business and ensure that the policies and strategies are effectively managed.

The composition, frequency and quorum shall be decided by the Board of Directors

Implementation

The implementation of this risk management policy shall be the responsibility of process owners and functional heads, who shall ensure that the risk management framework is effectively applied within their respective areas of operation.

They shall identify, assess, monitor, and mitigate risks relevant to their functions and ensure adherence to the internal controls and procedures established by the company.

The functional heads shall report key risk matters, exposures, and control deficiencies to the managing director or senior management, as may be applicable, for review and necessary action.

The managing director shall, in turn, place such risk-related information before the board of directors or the risk management committee, if constituted, for its review and noting

Board Approval and Review

i) The policy shall be approved by the Board of Directors of the Company.

ii) The Policy shall be reviewed by the Board at least **once in a year**, or earlier if required, to incorporate:

- Changes in regulatory requirements
- Modifications in business operations or risk profile
- Observations from internal audits or risk assessments
- Any significant risk events or control failures

iii) Any amendments to this Policy shall be subject to approval by the Board of Directors