RISK MANAGEMENT POLICY

Of

FDPL FINANCE PRIVATE LIMITED

(FFPL)

Approval Date	Version History	Approval Authority
15th Jan 2025	V-FY2501	Board of Directors
11th Sep 2025	V-FY2502	Board of Directors

CONTENTS

A. PREAMBLE

The Board of Directors ("Board") of FDPL Finance Private Limited ("the Company") recognizes that effective risk management is fundamental to the Company's long-term stability, financial soundness, and ability to serve its customers responsibly. In an evolving regulatory, economic, and technological environment, the Company is exposed to a range of risks including, but not limited to, credit risk, market risk, liquidity risk, operational risk, regulatory risk, reputational risk, and strategic risk.

This Risk Management Policy ("Policy") has been formulated to establish a structured and comprehensive framework for identifying, assessing, monitoring, and mitigating risks across all levels of the organization. It provides guiding principles and governance arrangements that ensure risks are managed in a proactive and consistent manner, in alignment with the Company's strategic objectives and its fiduciary duty to stakeholders.

The Policy is designed in accordance with:

- The Reserve Bank of India's *Master Direction – NBFC-Scale Based Regulation, 2023* (effective October 19, 2023), which supersedes the 2016 Master Directions and consolidates prudential and governance norms for NBFCs.
- The Reserve Bank of India's Guidance Note on Operational Risk Management and Operational Resilience dated April 30, 2024, which requires regulated entities to establish a robust Operational Risk Management Framework (ORMF) and ensure continuity of critical operations under severe but plausible scenarios.
- Good governance practices and globally accepted standards of risk management, including the principles outlined by the Basel Committee on Banking Supervision (BCBS).

The Policy underscores the Board's commitment to fostering a strong risk culture, embedding risk considerations into strategic and operational decision-making, and ensuring accountability across the "Three Lines of Defence" (business units, risk/compliance, and internal audit).

By adopting this Policy, the Company seeks to:

- Minimize adverse impacts on its financial condition, reputation, and operations.
- Strengthen resilience against both expected and unexpected events.
- Safeguard the interests of its customers, investors, lenders, and employees.
- Maintain compliance with applicable regulatory requirements.
- Enhance long-term stakeholder value through sound and sustainable risk management practices.

B. PURPOSE

The purpose of this Risk Management Policy is to define the objectives, scope, and intent of the Company's approach to risk management, ensuring that the risks are identified, assessed, managed, and monitored in a structured and consistent manner across all levels of operations.

This Policy is not merely a compliance requirement but an essential component of the Company's strategic and operational framework. It serves as the foundation for establishing and maintaining a comprehensive Risk Management Framework ('RMF') that safeguards the Company's assets, protects customer interests, ensures regulatory compliance, and promotes business resilience.

The specific purposes of this Policy are as follows:

- **Protection of Stakeholder Interests:** To protect the rights and interests of shareholders, customers, lenders, employees, and other stakeholders by minimizing the likelihood and impact of adverse events that may disrupt business continuity, erode financial performance, or impair reputation.
- **Alignment with Regulatory Expectations:** To ensure compliance with the Reserve Bank of India's regulations and specifically the Guidance Note on Operational Risk Management and Operational Resilience (April 30, 2024), by embedding operational risk management and resilience principles into day-to-day operations and decision-making.
- **Establishment of Risk Appetite and Tolerances:** To articulate the Board's Risk Appetite Framework ('RAF'), including measurable risk limits and tolerances, which will guide decision-making, risk acceptance, and escalation protocols throughout the Company.

- **Promotion of a Strong Risk Culture:** To cultivate a culture of accountability and awareness in which employees at all levels understand their responsibility for managing risk, adhere to ethical standards, and proactively identify and report risk events or vulnerabilities.
- **Enable Strategic Decision-Making:** To provide the Management and the Board with the necessary risk information, analytics, and tools to make informed strategic and operational decisions, balancing opportunities with associated risks.
- **Enhance Operational Resilience:** To ensure that the Company can deliver critical operations in the face of disruptions, by setting clear impact tolerances, mapping dependencies, strengthening third-party risk management, and conducting periodic resilience testing.
- **Continuous Improvement:** To establish mechanisms for ongoing monitoring, internal audit, lessons learned exercises, and independent reviews, so that the risk management framework evolves in line with emerging risks, market dynamics, and regulatory requirements.

Through this Policy, the Company reiterates its commitment to embed risk management into its corporate DNA, ensuring that risk considerations are not viewed as constraints but as enablers of sustainable growth and innovation.

C. PRINCIPLES

The Company recognizes that risk management must be embedded in its culture, strategy, and daily operations to be effective. The following principles shall govern the design, implementation, and continuous enhancement of the Risk Management Framework (RMF):

1. **Creation and Protection of Value**

   Risk management is not an isolated function but an integral part of the Company's value creation process. Effective risk management ensures that risks are anticipated, managed, and mitigated in a way that supports the achievement of strategic and financial objectives. By proactively managing risks, the Company seeks to protect stakeholder value, safeguard its reputation, and ensure sustainability of operations.

2. **Integration into Organizational Processes**

   Risk management shall be seamlessly integrated into all organizational processes, including strategy formulation, business planning, lending operations, credit approvals, treasury activities, technology development, human resources, and customer service. Risk considerations will be part of key decisions rather than afterthoughts, ensuring a proactive rather than reactive approach.

3. **Explicit and Informed Decision-Making**

   All material business decisions shall be guided by an explicit consideration of risk. The Company will employ structured methodologies such as Risk and Control Self-Assessments ('RCSAs'), Key Risk Indicators ('KRIs'), and scenario analysis to quantify and assess risks. These tools will provide the Management and the Board with clear visibility into the risk–return trade-offs, thereby enabling informed decision-making.

4. **Focus on Uncertainty and Emerging Risks**

   The Company acknowledges that risks often arise from uncertainties in the business environment, regulatory landscape, and technology ecosystem. Therefore, risk management will not only address current exposures but also focus on identifying emerging risks—such as cyber threats, climate-related risks, or regulatory changes—that could affect the Company's ability to achieve its objectives.

5. **Dynamic, Iterative, and Responsive**

   The Company recognizes that the risk landscape is dynamic. Risk management processes will therefore be iterative, with regular reviews and updates to methodologies, thresholds, and frameworks to ensure responsiveness to changes in the internal and external environment. Feedback loops, post-incident reviews, and lessons learned exercises will form an integral part of this dynamic process.

6. **Accountability through the Three Lines of Defence**

   Accountability for risk management will be distributed across the organization in line with the Three Lines of Defence (3LoD) model:

   - First Line: Business units own and manage risks within their activities.
   - Second Line: The independent risk management and compliance functions develop policies, monitor adherence, and challenge the first line.
   - Third Line: The Internal Audit function provides independent assurance to the Board on the effectiveness of the RMF.

7. **Transparency and Communication**

   Open communication of risks is critical to effective management. The Company will foster an environment where employees are encouraged to escalate risk issues without fear of retaliation. Further, risk information will be communicated accurately and promptly to internal stakeholders, regulators, and, where appropriate, external stakeholders, in line with the Disclosure Policy.

D. DEFINITIONS

For the purposes of this Policy, unless the context otherwise requires, the following terms shall have the meanings assigned to them:

- **"Board" :** The Board of Directors of FDPL Finance Private Limited ("Company"), collectively responsible for overall governance and oversight of the Company's risk management framework.
- **"Company" :** Refers to FDPL Finance Private Limited, its employees, branches, and all business units.
- **"Directors" :** Individual members of the Board of the Company.
- **"Policy" :** Refers to this Risk Management Policy as approved by the Board, together with any amendments or annexures.
- **"RBI" :** The Reserve Bank of India, as the primary regulator of the Company.
- **"Risk" :** The possibility of an adverse event or outcome that may have a negative effect on the achievement of the Company's objectives. Risk encompasses both quantifiable (measurable) and non-quantifiable (qualitative) aspects, and includes uncertainty.
- **"Risk Appetite" :** The aggregate level and types of risk that the Board is willing to accept in pursuit of the Company's strategic objectives. It provides boundaries for risk-taking and is expressed through qualitative statements and quantitative measures.
- **"Risk Tolerance" :** The acceptable level of variation relative to the achievement of specific objectives. It represents thresholds or limits within which the Company is prepared to operate.
- **"Operational Risk" :** The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events. This includes legal risks, regulatory risks, conduct risks, technology risks, cyber risks, and reputational risks, but excludes strategic and business risks.
- **"Operational Resilience" :** The ability of the Company to deliver critical operations through disruption, by anticipating, preparing for, responding to, and adapting to shocks and stresses. Operational resilience goes beyond risk management to emphasize continuity of key services under severe but plausible scenarios.
- **"Critical Operations" :** Those operations, services, or activities that, if disrupted, could pose material risk to the Company's financial viability, reputation, customers, counterparties, or the stability of the wider financial system. Critical operations are identified and approved by the Board.
- **"Impact Tolerance" :** The maximum level of disruption to a critical operation that the Company is willing to accept, in terms of duration, customer impact, and service quality, before there would be intolerable harm to the Company, its customers, or the financial system.
- **"Three Lines of Defence (3LoD)" :** The governance model for accountability in risk management, comprising:
  - First Line: Business units that own and manage risks.
  - Second Line: Independent risk management and compliance functions that oversee and challenge.

  - Third Line: Internal Audit, providing independent assurance on the effectiveness of governance, risk, and controls.
- **"Risk and Control Self-Assessment (RCSA)" :** A structured methodology through which business units identify, assess, and document risks and controls within their processes, evaluate control effectiveness, and record residual risks.
- **"Key Risk Indicators (KRIs)" :** Metrics used to provide an early signal of increasing risk exposure in various areas of the business. KRIs are forward-looking and aligned with the Company's risk appetite and tolerances.
- **"Scenario Analysis" :** A forward-looking technique used to assess the potential impact of severe but plausible events on the Company's risk profile, including its ability to remain within risk appetite and to continue critical operations.
- **"Near Miss" :** An event that had the potential to cause loss or disruption but did not result in actual loss, often due to timely intervention or chance. Recording near misses help strengthen preventive controls.
- **"Incident" :** An event (planned or unplanned) that disrupts normal business operations and requires a structured response. Incidents may include operational risk events such as frauds, system outages, regulatory breaches, cyberattacks, or natural disasters.
- **"Lessons Learned Exercise (LLE)" :** A structured review conducted after an incident or resilience test, with the objective of identifying gaps, deriving insights, and implementing corrective actions to strengthen the framework.
- **"Business Continuity Plan (BCP)" :** A documented framework that sets out procedures for maintaining or restoring critical operations during and after a disruption. It includes roles, responsibilities, recovery strategies, and communication protocols.
- **"Disaster Recovery (DR)" :** The process, policies, and tools related specifically to restoring IT systems, applications, and data following a disruption. DR is a subset of the BCP.
- **"Third-Party Service Provider" :** An external entity that provides goods or services to the Company. Where such services support critical operations, they must maintain resilience standards at least equivalent to those of the Company.

E. POLICY

The Company acknowledges that risk is inherent in all business activities and must be managed systematically to safeguard financial soundness, customer trust, and long-term stakeholder value. The purpose of this Policy is not to eliminate risk, but to ensure that risks are identified, assessed, monitored, and controlled within the Board-approved Risk Appetite Framework (RAF).

Through this Policy, the Company commits to:

- Embedding risk management into strategy, operations, and decision-making across all functions.
- Establishing a robust Operational Risk Management Framework (ORMF) covering risk identification, assessment, mitigation, monitoring, and reporting.
- Ensuring operational resilience by identifying critical operations, setting impact tolerances, and maintaining effective business continuity and third-party risk controls.
- Strengthening ICT and cyber resilience to protect data, systems, and customer interests.
- Implementing a structured incident management and lessons-learned framework for continuous improvement.
- Providing the Board and management with timely and accurate risk information to enable sound decision-making. To continuously thrive for available risks in the organization which directly or indirectly effect the functioning of the organization.
- To ensure the protection of rights & values of Shareholders by establishing a well-organized Risk Management Framework.
- Selecting, maintaining and enhancing the risk management tools used by the program to provide analyses that inform and support the investment actions of the entire organization.

This Policy applies to all employees, business units, and third parties engaged by the Company. The Board, assisted by the Risk Management Committee, shall review the Policy annually and update it as necessary to reflect regulatory changes, emerging risks, and evolving business requirements.

F. IDENTIFICATION, MEASUREMENT AND ASSESSMENT OF RISK

The objective of risk identification, measurement, and assessment is to establish a consistent, structured, and comprehensive process for recognizing risks across the Company, evaluating their potential impact, and ensuring that mitigation measures are proportionate and effective. This process forms the foundation of the Company's ORMF and underpins decision-making at all levels.

Risk Identification

Risks shall be identified across all business lines, functions, and processes using both top-down and bottom-up approaches:

- **Top-down:** Board and Senior Management will identify strategic and emerging risks (e.g., macroeconomic trends, regulatory changes, systemic events).
- **Bottom-up:** Business units will conduct Risk and Control Self-Assessments (RCSAs) to identify process-level risks, control weaknesses, and vulnerabilities.
- **Sources of risk information:** Internal audits, compliance reviews, whistle-blower reports, customer complaints, IT incident logs, HR records, external loss databases, industry benchmarking, and regulatory circulars.
- **Risk taxonomy:** All risks will be recorded in line with the Company's standardized taxonomy (credit, market, liquidity, operational, compliance, reputational, strategic, etc.).

Each identified risk shall be recorded in the Central Risk Register, along with:

- Risk description.
- Root cause(s).
- Potential impact.
- Current controls in place.
- Residual risk assessment.
- Risk owner (first line of defence).

Risk Management

The Company shall apply both quantitative and qualitative techniques to measure risks:

- **Likelihood and Impact Ratings:** All risks will be scored on the basis of likelihood (probability of occurrence) and impact (financial, operational, reputational, and regulatory consequences).
- **Scoring Matrix:** A standard 5x5 likelihood–impact matrix will be used to categorize risks as low, medium, high, or critical.
- **Financial Quantification:** Where feasible, risks will be expressed in terms of potential financial loss or earnings-at-risk.
- **Control Effectiveness:** The strength of existing controls will be assessed to determine residual risk levels.

Risk Assessment Tools

The following tools will form part of the Company's ongoing assessment methodology:

- **Risk and Control Self-Assessment (RCSA):** Conducted periodically by business units, reviewed by the second line, and approved by the Risk Management Committee.
- **Key Risk Indicators (KRIs):** Defined metrics (e.g., loan delinquency ratios, IT downtime hours, fraud incidents) with thresholds linked to the Board-approved risk appetite. Breaches will trigger escalation and corrective action.
- **Operational Loss Database:** A repository capturing all operational risk events, including losses, near misses, and external events. The database will record event type, amount, cause, corrective action, and lessons learned.
- **Scenario Analysis:** Stress testing of severe but plausible scenarios (e.g., cyber-attack, prolonged IT outage, natural disaster, regulatory penalty) to assess resilience and inform capital planning.

Risk Aggregation and Reporting

Risk assessment results shall be aggregated and presented to the Management and the Board through dashboards and MIS reports, including:

- Risk profile by business line and category.
- Emerging risks and trend analysis.
- High residual risk items and mitigation status.
- KRI breaches and corrective actions.
- Loss event data and lessons learned.

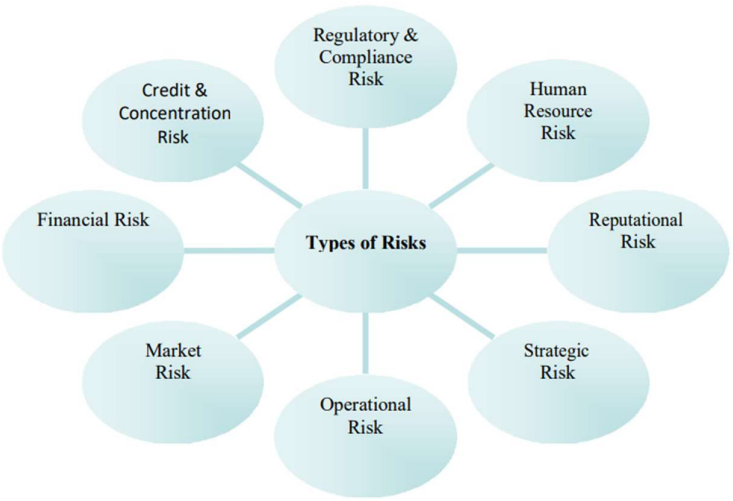
Reports shall be prepared monthly for senior management and quarterly for the Risk Management Committee and Board.

Independent Review

The Internal Audit function (third line of defence) shall independently review the risk identification and assessment process at least annually to ensure accuracy, completeness, and effectiveness.

G. Risk Categorization and Mitigation Factors

The Company recognizes that risks arise from multiple sources, both internal and external, and can affect different dimensions of the business. To ensure comprehensive coverage, risks are categorized into broad classes. Each category is described below along with its mitigation strategy, governance arrangements, and monitoring mechanisms.



1. Strategic Risk:

Definition: Strategic risk is the potential for adverse impact on earnings and capital, arising from inappropriate business decisions, inadequate responsiveness to changes in the external environment, or failure to implement chosen strategies effectively. It may also stem from misalignment between the Company's strategy and market conditions.

Examples: Wrong product-market choices, entry into unsuitable geographies, excessive reliance on a single segment, failure to respond to fintech disruptions, or regulatory changes that make a business line unviable.

Mitigation Measures:

- Annual strategic planning exercise with scenario analysis and Board review.
- Periodic market and competitor analysis to ensure continued relevance.
- Approval of significant strategic initiatives by the Board or its committees, supported by independent evaluation.
- Maintenance of Directors' and Officers' Liability Insurance to protect decision-makers when acting in good faith.
- Continuous monitoring of macroeconomic, political, and regulatory developments.

2. **Operational Risk**

Definition: The risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events, including fraud, cyber incidents, and natural disasters.

Examples: Fraudulent transactions, system outages, errors in loan processing, information security breaches, employee misconduct, or disruption in service delivery.

Mitigation Measures:

- Risk and Control Self-Assessments (RCSAs) conducted by all departments.
- Proper storage of documents and appropriate system for retrieval. The Company shall maintain all the original documents in a dedicated space allocated for specific purpose.
- Maintain scanned copies of the loan documents, statutory documents / papers / certificates, KYCs of all employees including Directors, KYCs of all customers for easy retrieval especially for audit purposes where physical documents are not required.
- A Whistle-Blower Policy encouraging employees to report any instances or suspected instances of violation of the Code, malpractice, corruption, fraud or unethical conduct, leakage or suspected leakage of Unpublished Price Sensitive information of the Company.
- Internal Audits at both branch and head office levels, covering all operational processes, to be carried out periodically.
- Information Technology controls, including secure access, regular system audits, anti-virus protection, and periodic cybersecurity assessments. The scope of this Internal Audit shall cover all key functions including HR, Operations, Credit, Administration, Finance and Accounts. All significant audit observations of Internal Audits and follow-up actions shall be presented to the Board.
- Technology Infrastructure: The Company has a fully computerized environment for conducting its business operations. The database server gets updated online. Only authorized personnel will have access to the data base. Scope to tamper or alter the database will be eliminated through controls. A secured system of access control, both on-site and remote, including password management and secrecy will be in place and reviewed periodically. Suitable antivirus software will be loaded in the central server and at all user points and updated regularly. A regular 'system audit' will be conducted to cover both hardware and software and the irregularities immediately addressed. An efficient system to report and manage IT incidents and problems will be in place across the network of branch offices.
- Business Continuity Plan (BCP) and Disaster Recovery (DR) framework with periodic testing.
- Adequate insurance coverage for operational losses where feasible.
- Continuous staff training in operational controls, information security, and customer service.

3. **Market Risk:**

Definition: The risk of financial loss arising from adverse movements in market variables such as interest rates, foreign exchange rates, or asset values.

Examples: A sudden increase in borrowing costs, currency depreciation affecting foreign borrowings, or fall in the value of investments. Risks relating to inherent characteristics of our industry including competitive structure, technological landscape, extent of linkage to economic environment and regulatory structure.

Mitigation Measures:

- Periodical Asset-Liability Management (ALM) analysis to assess exposures.
- Use of hedging instruments permitted by RBI, including swaps and options, for interest rate and forex exposures.
- Diversification of investment portfolios and monitoring of market trends.
- Stress testing for interest rate shocks and liquidity disruptions.
- Regular competitive analysis of its peers in the industry so as to remain in competition and change its markets if required.

4. **Financial Risk:**

Definition: The risk of losses from factors impacting the Company's balance sheet and financial performance, including liquidity risk, leverage risk, and capital adequacy concerns.

i **Interest Rate Risk:**
Interest rate risk is the risk where changes in market interest rates might adversely affect an NBFC's financial condition. The changes in interest rates affect company in some way. The immediate impact of changes in interest rates is on company's earnings by changing its Net Interest Income (NII). The Company shall manage this risk on NII by pricing its loan products to customers at a rate which covers interest rate risk. The risk from the earnings perspective can be measured as changes in the Net Interest Income (NII) or Net Interest Margin (NIM). Measurement of such risk shall be done at the time of deciding rates to be offered to customers. Once interest rate risk is measured, lending rates shall be finalized. Given the interest rate fluctuation, the Company shall adopt a prudent & conservative risk mitigation strategy to minimize interest risk.

ii **Foreign Exchange Risk:**
The Company may get exposed to variation in foreign exchange rates on account of its borrowings in foreign currency and change of interest rate on foreign currency borrowings. The change in foreign exchange rates has a direct impact on Company's financials and its competitiveness. The policy lays down the tools that are permitted to be used for hedging of various risks by Company's treasury. The Company shall use only those hedging tools that are permitted by RBI from time to time. In addition to that the said tools must be permitted under the risk management policy.

iii **Liquidity Risk:**
Measuring and managing liquidity needs are vital for effective operations of an NBFC. The importance of liquidity transcends individual institutions, as liquidity shortfall in one institution can have repercussions on the entire system. Board shall measure not only the liquidity positions of company on an ongoing basis but also examine how liquidity requirements are likely to evolve under different assumptions. Experience shows that assets commonly considered as liquid, like government securities and other money market instruments, could also become illiquid when the market and players are unidirectional. Therefore, liquidity has to be tracked through maturity or cash flow mismatches. For measuring and managing net funding requirements, the use of a maturity ladder and calculation of cumulative surplus or deficit of funds at selected maturity dates shall be adopted as a standard tool. Due to the high reliance on external sources of funds, Company may get exposed to various funding and liquidity risks comprising:

- **Funding Concentration Risk:** Concentration of a single source of funds exposes the Company to an inability to raise funds in a planned and timely manner and resort to high cost emergency sources of funds. Further, concentration of funding sources can also result in a skewed maturity profile of liabilities and resultant Asset-Liability mismatch.
- **Asset-Liability Mismatch:** A skewed asset-liability profile can lead to severe liquidity shortfall and result in significantly higher costs of funds; especially so **during** times of crises.
- **Market Perception Risk**: Due to inherent industry characteristics, the Company may get exposed to perception risks, which can lead to decline in ability of a lender to increase exposure to the Asset Finance -two wheeler and MSME sector and result lack of adequate and timely inflow of funds.
- **Leverage Risk:** A high degree of leverage can severely impact the liquidity profile of the Company and lead to default in meeting its liabilities.

Mitigation Measures:

- Maintenance of a Liquidity Risk Management Policy, including cash-flow forecasting, maturity gap analysis, and contingency funding plans.
- Monitoring of funding concentration to avoid over-reliance on a single source or lender.
- Target leverage ratio as approved by the Board from time to time.
- Prudent capital planning to ensure capital adequacy remains well above regulatory minimums.
- Maintenance of committed credit lines and access to multiple funding sources.
- The key liquidity management policies shall be followed at Company include:
  - ALM Meetings: This shall be done to identify any short term / long term liquidity gaps and thereby take immediate corrective actions to bridge the same.
  - Lender Exposure Updates: The exposure profile to the lenders shall be regularly updated to ensure that skewness does not creep in in respect of the sources of external funds.
  - Floating Rates: Company currently borrows all its loans on a floating basis as against the entire lending on a fixed rate basis. This minimizes the impact of any adverse impact in the event of a credit shock in the banking system and any continuing effects of the same on overall interest rates in the economy and on Company.
  - Defined Leverage Levels: Company shall target a leverage ratio (as approved by the Board from time to time) in light of the business model and adequately safeguard itself against the impact of adverse market conditions. It also affords Company reasonable time to tie-up timely equity infusion. o Hedging on forex borrowing: The Company might use following tools for hedging which are currently prevailing in the market:
    ♣ Foreign Currency - INR Options
    ♣ Foreign Currency – to – INR Swaps
    ♣ INR – to – Foreign Currency Swaps
    ♣ Cost Reduction Structures
    ♣ Interest Rate Swap
    ♣ Cross currency swap, and its variations such as Coupon swap, Principal Only Swap
    ♣ Interest rate cap or collar (purchases), Forward rate agreement (FRA)
    ♣ Exchange Traded Hedge Contracts
    ♣ Combination of above permitted instruments which are combination of either cash instrument and one or more generic derivative products; or instruments which are combination of two or more generic derivative products

    While applying above tools, the Company shall ensure that:
    ♣ The maturity of the hedge shall not exceed the maturity of the underlying transaction.
    ♣ The notional of the hedge shall not exceed the notional of the underlying transaction.

    The execution of hedges shall be done only by designated employees of the Company. The execution of hedges shall only be done with the banks permitted by RBI. The Authorised person executing hedging transactions shall follow the guidelines prescribed by RBI for that purpose and shall report to the management on a monthly basis.

- **Capital Adequacy:** Company shall target to maintain healthy levels of capital adequacy. The Company shall maintain a strong capital position with the capital ratios well above the thresholds defined by the regulatory authorities through continuous and timely capital infusion.

5. **Credit and Concentration Risk:**

Definition: The risk of loss due to the failure of customers to meet their contractual obligations, or due to excessive exposure to a single borrower, industry, geography, or product.

Examples: Loan defaults, downgrades in credit ratings, excessive exposure to a single sector such as MSME, or high concentration in a particular state or region.

Mitigation Measures:

- Structured and standardized credit approval process supported by underwriting standards, due diligence, effective training programs, and independent verification.
- Regular portfolio monitoring through early warning signals, stress testing, and vintage analysis.
- Use of third-party agencies for legal, technical, and valuation assessments.
- Diversification across industries, sectors, geographies, and customer segments.
- Implementation of credit risk limits at borrower, group, and sector levels, reviewed quarterly by the Board.

6. **Regulatory and Compliance Risk:**

Definition: The risk of legal or regulatory sanctions, material financial loss, or reputational damage arising from failure to comply with applicable laws, regulations, codes of conduct, or supervisory expectations.

Examples: Non-compliance with RBI regulations / statutory regulations / covenants laid down by the Lenders

Mitigation Measures:

- Implementation of a Compliance Management System to track and monitor compliance obligations.
- Appointment of a Compliance Officer with direct reporting to the Board.
- Quarterly certification by the CEO and Company Secretary confirming compliance status.
- Periodic regulatory audits by external firms.
- Training programs for staff on compliance obligations (RBI directions, fair lending practices, data protection, etc.).

7. **Human Resource Risk**

Definition: Risks arising from inadequate HR policies, talent shortages, poor employee engagement, safety issues, or unethical conduct.

Company's Human Resource adds value to the entire Company by ensuring that the right person is assigned to the right job and that they grow and contribute towards organizational excellence. Our growth has been driven by our ability to attract top quality talent and effectively engage them in right jobs. Risk in matters of human resources are sought to be minimized and contained by following a policy of providing equal opportunity to every employee, inculcate in them a sense of belonging and commitment and also effectively train them in spheres other than their own specialization. Employees are encouraged to make suggestions on innovations, cost saving procedures, free exchange of other positive ideas etc. It is believed that a satisfied and committed employee will give of his best and create an atmosphere that cannot be conducive to risk exposure. Employee compensation is always subjected to fair appraisal systems with the participation of the employee and is consistent with job content, peer comparison and individual performance.

Mitigation Measures:

- Comprehensive Human Resource Policy covering recruitment, training, performance appraisal, and succession planning.
- Employee engagement and retention initiatives, including ESOP schemes for key staff.
- Provision of health and accident insurance for employees.
- Promotion of a fair and inclusive workplace culture with equal opportunities.
- Periodic employee satisfaction surveys to identify emerging issues.

8. **Reputational risk:**

Definition: The risk of negative perception among stakeholders—customers, regulators, investors, or the public—that could adversely affect the Company's ability to conduct business. It refers to the potential adverse effects, which can arise from the Company's reputation getting tarnished due to factors such as unethical practices, regulatory actions, customer dissatisfaction and complaints leading to negative publicity. Presence in a regulated and socially sensitive industry can result in significant impact on Company's reputation and brand equity as perceived by multiple entities like the RBI, Central/State/Local authorities, banking industry and the customers.

Examples: Customer dissatisfaction, media criticism, unethical recovery practices, data breaches, regulatory penalties.

Mitigation Measures:

- Strict adherence to Fair Practices Code and ethical conduct standards. All employees shall be trained and instructed to follow fair practices as per RBI prescribed guidelines in all their dealings with the customers.
- Transparent Grievance Redressal Mechanism (GRM), communicated at loan sanction and displayed on the website.
- Clear Code of Conduct outlined in the Outsourcing Policy prohibiting coercive practices. All recoveries shall be made in accordance with the Recovery policy and Fair Practice Code of the Company.
- Vetting of vendors, employees, and associates against reputational risks before onboarding.
- Inclusion of confidentiality and non-disclosure clauses in contracts with third parties.
- Continuous monitoring of public perception through customer feedback and media scanning.

H. RESPONSIBILITY & GOVERNANCE

Risk management is the responsibility of every individual within the Company. However, accountability must be clearly defined and distributed to ensure that risks are managed systematically and consistently across the organization. The governance structure is built on the principle of the Three Lines of Defence (3LoD) and ensures effective oversight by the Board and its committees.

Board of Directors

The Board holds ultimate responsibility for risk governance. Its duties include:

- Approving the Risk Management Policy and the Risk Appetite Framework (RAF), including limits and tolerances.
- Reviewing and approving the ORMF, including identification of critical operations and their impact tolerances.
- Ensuring adequate resources and independence of the risk management and compliance functions.
- Monitoring adherence to the risk appetite and reviewing significant breaches or emerging risks.
- Overseeing the Company's operational resilience, including BCP, DR, and third-party risk management.
- Ensuring that Senior management fosters a strong risk culture throughout the organization.
- Approving public disclosures relating to risk management and resilience in line with regulatory requirements.

The Board may delegate detailed oversight responsibilities to its committees, while retaining overall accountability.

Risk Management Committee (RMC)

The RMC, established in line with RBI guidelines, supports the Board in risk oversight. Its responsibilities include:

- Reviewing and recommending the risk appetite statement and key risk policies to the Board.
- Monitoring the Company's risk profile across all categories—credit, market, liquidity, operational, compliance, strategic, reputational.
- Reviewing the Central Risk Register, KRIs, and results of RCSAs and scenario analysis.
- Reviewing reports on significant risk events, control deficiencies, and remediation actions.
- Overseeing change management processes for new products, services, and markets.
- Ensuring integration of risk management into strategic planning and capital allocation.
- Reporting key risk issues and recommendations to the Board on a quarterly basis.

Audit Committee

The Audit Committee ensures independent assurance over the risk management framework. Its responsibilities include:

- Reviewing the adequacy and effectiveness of internal controls and audits.
- Reviewing audit findings on operational risk, compliance, and IT/cybersecurity.
- Monitoring implementation of corrective actions by management.
- Reviewing quarterly and annual financial statements for risk disclosures.
- Escalating significant control deficiencies or audit concerns to the Board.

Senior Management

Senior Management, led by the Executive Director/s, is responsible for implementing the Board-approved risk management framework. Their responsibilities include:

- Operationalizing the ORMF and ensuring it is embedded in business processes.
- Establishing the Central Risk Register and maintaining risk event and loss data.
- Implementing RCSA, KRIs, and scenario analysis programs across business units.
- Monitoring risk exposures against approved limits and tolerances.
- Ensuring adequacy of ICT and cybersecurity controls.
- Coordinating resilience activities including BCP/DR drills and third-party dependency reviews.
- Ensuring effective incident reporting, investigation, and Lessons Learned Exercises (LLEs).
- Reporting risk exposures, tolerance breaches, and mitigation actions to the RMCB and the Board.

Three Lines of Defense

I. First Line of Defence – Business Units

- Own and manage risks inherent in their day-to-day activities.
- Identify, assess, and report risks through RCSAs and KRIs.
- Implement controls and ensure compliance with policies.
- Escalate issues and breaches promptly to Senior Management and the second line.

II. Second Line of Defence – Risk Management & Compliance Functions

- Develop risk policies, frameworks, methodologies, and tools.
- Provide independent monitoring, review, and challenge of the first line.
- Track and report risk exposures, tolerance breaches, and emerging risks.
- Ensure compliance with applicable laws, regulations, and internal policies.
- Facilitate risk awareness training across the Company.

III. Third Line of Defence – Internal Audit

- Provide independent and objective assurance to the Board and Audit Committee.
- Review adequacy and effectiveness of the risk management framework, internal controls, and governance arrangements.
- Validate risk reports and ensure completeness and accuracy of risk data.
- Conduct thematic audits on emerging or high-risk areas.

Employees

Every employee is responsible for adhering to this Policy and for exercising due care in their respective roles. Employees are expected to:

- Understand the risks associated with their activities.
- Comply with all internal policies, procedures, and controls.
- Promptly report operational issues, control weaknesses, or suspicious activities through designated channels, including the Whistle-Blower mechanism.
- Contribute to building a risk-aware culture within the organization.

Independent Assurance

Independent reviews of the risk management framework will be carried out through:

- Internal Audit reviews (quarterly and annual).
- External audits and regulatory inspections as required.
- Independent validation of risk models, methodologies, and IT systems.

Findings will be reported to the Audit Committee and the Board with timelines for remediation.

I. CHANGE MANAGEMENT

The Company recognizes that new products, services, processes, or systems can significantly influence its risk profile. A structured Change Management Framework has therefore been established to ensure that all changes are evaluated, approved, and monitored before implementation. This ensures that innovation and growth are pursued responsibly without compromising the Company's risk appetite or resilience.

The framework applies to all new loan products, customer segments, technology systems, material process changes, and market entries. Every proposal must be accompanied by a documented risk assessment that considers inherent risks, required controls, and residual risks.

Approval: Routine changes of low impact may be approved by Senior Management. Material changes must be reviewed by the Risk Management Committee and approved by the Board.

Documentation: A central register of all new products, services, and material changes will be maintained, capturing risk assessments and approval decisions.

Post-Implementation Review: Within 6–12 months of implementation, each material change shall be reviewed to evaluate its effectiveness, risk outcomes, and any emerging issues.

Post-Implementation Review: Within 6–12 months of implementation, each material change shall be reviewed to evaluate its effectiveness, risk outcomes, and any emerging issues.

J. OPERATIONAL RESILIENCE

Operational resilience is the ability of the Company to deliver its critical operations even under conditions of severe disruption. It extends beyond traditional risk management by focusing on continuity of essential services that customers, regulators, and the wider financial system depend upon.

The framework for operational resilience rests on the following pillars:

- **Identification of Critical Operations:** The Board will approve a list of services whose disruption could pose material harm to the Company or its stakeholders.
- **Impact Tolerances:** For each critical operation, maximum tolerable levels of disruption will be defined (e.g., downtime, number of customers affected).
- **Dependency Mapping:** All supporting people, processes, technology, facilities, data, and third parties will be mapped to identify single points of failure.
- **Resilience Testing:** Severe but plausible scenarios (e.g., cyber-attack, IT outage, natural disaster) will be simulated to validate resilience.
- **Integration with BCP/DR:** Business Continuity and Disaster Recovery plans will align recovery objectives with the Board-approved impact tolerances.

Through this approach, the Company seeks to ensure that its critical operations remain available, reliable, and trusted even during unforeseen shocks.

K. ICT and Cybersecurity

The Company acknowledges that technology is both an enabler of growth and a source of risk. With increasing reliance on ICT systems, robust cybersecurity and IT resilience have become fundamental to operational risk management.

The Company's ICT and Cybersecurity framework is guided by the following principles:

- **Governance:** A Board-approved ICT & Cybersecurity Policy is maintained, with Senior Management responsible for its implementation and oversight.
- **Access Management:** Strong authentication protocols, restricted privileged access, and secure password practices are enforced.
- **Data Protection:** Customer and Company data are protected through encryption, secure backups, and data loss prevention tools.
- **Monitoring and Detection:** Intrusion detection, vulnerability assessments, penetration testing, and continuous monitoring are carried out regularly.
- **Incident Response:** A predefined cyber incident response plan ensures timely containment, investigation, and regulatory reporting.
- **Resilience:** Offline, immutable backups and stress testing of system capacity and remote access are maintained to withstand shocks.
- **Third-Party Oversight:** ICT service providers and vendors are required to maintain standards of resilience and cybersecurity equivalent to the Company's own.

L. INCIDENT MANAGEMENT

Disruptions, whether internal or external, require a structured and consistent response. The Company has established an Incident Management Framework to ensure that incidents are managed promptly, transparently, and with clear accountability.

The framework encompasses the full lifecycle of incident handling:

- **Identification and Classification:** All incidents, including operational losses, cyber events, frauds, or process failures, must be logged and classified by severity (low, medium, high, critical).
- **Escalation:** Material or critical incidents are escalated immediately to Senior Management, the Risk Management Committee, and regulators where required.
- **Response and Recovery:** Predefined playbooks guide response teams in containing the incident and restoring services, including activation of BCP/DR where necessary.
- **Communication:** Internal and external communication protocols ensure accurate and timely updates to staff, customers, and regulators.
- **Closure and Lessons Learned:** Post-incident reviews (LLEs) are conducted to identify root causes, evaluate control effectiveness, and track corrective actions.

M. LESSONS LEARNED AND CONITNUOUS IMPROVEMENT

The Company views every incident, disruption, and resilience test as an opportunity to strengthen its framework. A structured Lessons Learned Exercise (LLE) is conducted after significant events to analyze what went wrong, what worked well, and what must be improved.

Key features include:

- Root cause analysis of the incident.
- Evaluation of the adequacy of controls and response measures.
- Recording of insights in a centralized Remediation Tracker.
- Assignment of ownership for corrective actions, with timelines monitored by the Risk Management Committee.
- Dissemination of lessons across business units to prevent recurrence.

N. DISCLOSURES & TRANSPARENCY

Transparency in risk management is essential for maintaining trust with customers, investors, regulators, and other stakeholders. The Company has therefore adopted a Disclosure Policy which governs the scope, process, and frequency of disclosures relating to its risk framework and resilience practices.

The Company commits to disclose, at a minimum:

- The governance structure of risk management, including Board oversight and committees.
- A description of the ORMF.
- Information on critical operations and the approach to operational resilience.
- Summary of key risk exposures and mitigation strategies.
- Significant operational risk events, where disclosure is required by law or regulation.

Disclosures shall be reviewed annually by the Board to ensure accuracy, completeness, and alignment with evolving regulatory requirements. The Company will balance the need for transparency with the need to safeguard sensitive information that, if disclosed, could create additional risks.

O. AMENDMENTS:

This policy may be amended subject to the approval of Board of Directors, from time to time in line with the business requirement of the Company or any statutory enactment or amendment thereto.