MANAPPURAM ASSET FINANCE LIMITED

ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK

Version Control		
Version Number	**Description**	**Date**
Version 1.0	Risk Management Policy	09-08-2013
Version 2.0	Risk Management Policy	07-02-2014
Version 3.0	ERM Policy & Framework	27-02-2025
Version 4.0	ERM Policy & Framework	21-03-2026

Effective Date	**21-03-2026**
Review	**Yearly**
Policy Owner	**Risk Management Department**
Prepared By	**Risk Management Department**
Reviewed by	**Policy Review Committee**
Approved By	**Board**

Contents

Introduction

Manappuram Asset Finance Ltd. (MAAFIN) has been in the business of gold loans from 1987. While the core business of the Company continues *to be* Gold Loans, currently the company offers a diversified product portfolio including gold loans, MSME / SME finance, vehicle and equipment finance, personal loans, home improvement loans.

The policy was updated with more features like reputation risk management, liquidity risk management, cyber security, ICAAP etc. Further, this policy should also be read in conjunction with various Master Directions, which inter alia include the following:

A. Credit Risk Management.

B. Operation Risk Management.

C. Liquidity Risk Management.

D. Outsourcing (Financial Services). E. Outsourcing (IT)

F. Reputation Risk Management.

G. Market Risk Management Policy (viz. ALM, Resources Management).

1.1 What is Enterprise Risk Management

Enterprise Risk Management (ERM) is defined by the Committee of Sponsoring

Organizations (COSO) as "a process, effected by an entity's Board of Directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Integration with Strategy and Performance, the Company recognizes that a strong Risk Culture forms the foundation of an effective ERM framework. Risk culture reflects the shared values, attitudes, competencies, and behaviors that influence how risk is identified, understood, discussed, and managed across the organization. The Company shall promote a risk-aware culture by embedding accountability, ethical conduct, and risk-informed decision-making into all business activities and performance management frameworks, including alignment with Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs).

The Company adopts this globally accepted definition and will be guided by the philosophy eschewed thereunder.

2. Objective of this Policy

The main objective of the policy is to keep the Board of Directors and Top Management apprised of the applicable risks promptly and regularly.

This risk management policy aims, among other things, to protect the reputation of the organization, enabling the Company to make consistently profitable and prudent business decisions across all its offices and ensure an acceptable Risk-Adjusted Return On Capital (RAROC), Risk-Appetite based Risk-Tolerances (including defined Risk Limits as applicable) and to be within its overall risk capacity or any other equivalent measure.

In a nutshell, it seeks to ensure sustainable growth with profitability within the Company's risk absorption capacity, supported by robust capital planning and stress testing frameworks, while maintaining strong governance and compliance standards.

3. Risk Management Approach

Pillars of ERM

As mentioned, Enterprise Risk Management (ERM) looks at risk Management from the perspective of the entire organization. It identifies and assesses potential losses, dangers, hazards, and other potentially harmful factors that may prevent the organization from achieving its objectives. Appropriately applied, ERM supports sound decision-making and offers sound risk responses in today's volatile, dynamic and uncertain business environment.

ERM is founded on four pillars: Risk Identification and assessment; risk response; control activities and monitoring; and information, communication and reporting. All ERM frameworks must encompass these four pillars, to be truly effective organizational strategy.

1. **Sound risk Identification and assessment**: This requires to be done systematically so that the company is able to clearly understand as to what its risks are and manage them accordingly.it is possible that not all the risks that the company is exposed to may be similar to peer groups in the industry but may vary based on several internal and other relevant factors in which we operate.
2. **Responding to identified risks**: Once the risk universe has been identified and assessed, it is necessary to develop risk management plans for risk mitigation. The process of identification and assessment may indicESG Sate a need for tighter internal controls and possible opportunities that may be a benefit to the firm.
3. **Control activities and monitoring**: This pillar covers establishing and maintaining internal controls that manage and monitor risks.
4. **Information, communication and reporting**: This pillar focuses on establishing clear lines of communication between the Company and its stakeholders, which may include shareholders, employees, customers, suppliers, regulators and communities where the firm operates. Information needs to be verifiable and reliable, to be useful, and reporting must be accurate and timely to support informed decision-making. Additionally, clear communication, data with integrity and timely reporting enhance the Company's commitment to transparency.

While traditional risk management tends to leave decision-making with individual business units or division heads, this may create a siloed approach that will not be as effective as the integrated approach inherent with ERM, which approaches risk management holistically. ERM promotes a big picture view and facilitates an understanding of how risks to individual

business units are interconnected. This allows it to identify potential risk factors that may not be obvious to individual units; information like this allows management to decide which risks should be actively managed, whilst at the same time allowing each business unit to be responsible for its own risk management.

Communication is key in the integration and successful implementation of ERM. While ERM practices will normally vary based on company size, risk preferences and business objectives, applying this approach allows the firm to optimize risks throughout its structure while identifying opportunities for individual business units and the firm as a whole. Regardless of the type of risk faced, ERM is intended to ensure a firm's competitiveness, growth and sustainability.

4. Risk Management - The New and Strategic Approach

The strategic approach to Risk Management includes a detailed study of the Economic environment through scanning of national (and international) data as appropriate to assess and identify imminent risks and potential opportunities.

Typically, the Strategic part of Enterprise Risk Management will consist of an analysis of the External environment and Internal Assessments:

Analysis of the External Environment would normally include the following:

1. **Economic Risk**
    a. Macro-Economic Indicators affecting our businesses
    b. Microeconomic Indicators influencing our businesses
2. **Strategic Analysis**
    a. Business Analysis – including Industry Analysis
    b. Forecasting & Modelling – including techniques and thresholds
    c. Statistical Analysis – indicative and prescriptive

5. Risk Management – The Conventional Approach

Having recognized the "conventional" approach of 'structured risk management practices' would be bedrock on which the higher-level approaches can function effectively and given the fact that the Company has already adopted to follow the BASEL GUIDELINES in managing its risks, the company will continue this approach to the 'conventional risk management' practice.

Traditionally, risks of an organization have been classified into the broad categories of

- Credit Risks
- Market Risks

- Operational Risks.
- Liquidity Risks

The company has a 5th Category called “Other Risks” which typically includes those not categorized into the above 4 buckets but are recognized as significant enough to be managed in a structured manner.
The following are the guidelines on what these risks are and how the company will manage them.

5.1 Credit Risk:

5.1.1 Definition

Credit Risk is defined as the "risk of failure of the borrower in keeping up its commitments. It can be further described as,

A credit risk is the risk of default on a debt that may arise from a borrower failing to make required payments. In the first resort, the risk is that of the lender and includes lost principal and interest, disruption to cash flows, and increased collection costs.

5.1.2 Status and Vision for Way Forward:

5.1.2.1 Current Status:

Credit risk –for the company’s core-business of Gold Loans - is perceived to be relatively lower due to the fully secured nature of loans.
While it is primarily a “fully secured” proposition, it is also recognized that risk is inherent due to the criticality of the value of collateral, more so when theft and spurious gold jewellery /Ornaments /Coins are pledged. The degree of comfort will depend on the Loan to Value (LTV) at which loan is sanctioned followed by subsequent price movements. Significant downward movement in the gold prices especially when interest accrued there on is not serviced, can impact the Company’s financials significantly.

The Company generally extends gold loans for a maximum tenor of 1 year, which is essentially short-term. Interest rates to be charged on the gold loans are fixed from time to time based on the overall cost of borrowings/funds from the various funding sources, cost of operations, Risk Premium, Liquidity Premium/Spread.

5.1.2.2 Way Forward:

However, with ambitious goals to achieve and with a vastly diversified portfolio (which proposes to include both secured- and un secured lending under the Micro, Small & Medium Segment (MSME), Retail and Commercial Loans for Vehicles, Personal Consumption, etc.) to be managed, it is imperative that the risks are managed by introducing stringent credit purveyance processes that encompass the entire gamut of the Credit Life cycle as follows: –

- sourcing of the right clientele,
- structuring products that would suit the selected markets / geographical and demographical profiles,

- credit assessment/appraisal processes, including adoption of structured score cards for decision making and adoption of external ratings for assessment of borrower ratings,
- credit administration processes that match the best in the industry,
- credit recovery strategies and processes that ensure minimal losses to the company while ensuring borrower rights are always protected, through the strengthening of the credit risk management team in the company.

5.1.3 Credit Risk – Objective

The objective of credit risk management is to ensure the overall health of the credit portfolio through an evaluation of the credit processes, credit worthiness of each customer, new or existing, assessment of the risks involved, and ensuring a measured/structured approach to address the risks.

Credit risk in gold loans is managed through a strong dual combination of collateral valuation and timely action on non-performance of the loan arrangement.

Credit risk management for other segments will include periodic portfolio reviews, continuous review of the existing controls, and monitoring of the systems for identification and mitigation of the various risk factors.

5.1.4 Credit Risk Management

The company at all times has a well-structured Risk Management Policy and Procedure that is duly supported by the Top Management and approved by the Board of Directors or by a committee appointed by them.

5.1.4.1 Introduction & Scope of the Credit Risk Management

The Risk Management Policy should set out the guidelines, principles, and approach to manage credit risks in the company and contain a framework to identify, assess, measure, monitor, and control credit risks in a timely and effective manner.

5.1.4.2 Objective

The Policy will always aim to achieve the following key objectives:

i. Establish a governance framework to ensure effective oversight, segregation of duties, monitoring, and management of credit risk in the company.
ii. Lay down guiding principles for setting up & monitoring the credit risk appetite & limits.
iii. Establish standards for an internal credit scoring framework
iv. Establish standards for effective measurement and monitoring of credit risk.
v. Achieve a well-diversified portfolio enabled by obviating concentration risk management and maintaining credit risk exposures within established credit limits.
vi. Establish principles for credit risk stress testing.
vii. Enable monitoring of credit risk by way of Early Warning Signals (EWS).

viii. Adhere to the guidelines/policies related to credit risk management, as issued by the Reserve Bank of India (RBI) from time to time.

5.2 Market Risk

5.2.1 Definition

Market Risk is defined as the risks arising from movements in interest rates, and underlying security value on the overall business of the company.

Even though the Company does not on its own account take 'open position' in the gold market, risk is inherent due to the criticality of the value of collateral. The degree of comfort will depend on the Loan to Value at which the loan is sanctioned, followed by the subsequent price movements. Significantly downward movement in the gold prices, especially when accompanied by non-servicing of interest, can impact the Company's financials significantly.

In terms of other loans (Business Loans, Loan Against Immovable Property & Vehicle Loans) with maturity from 3 to 10 years, price rate risk is relatively low, unless some fraudulent and malfeasant transactions occur.

5.2.2 Liquidity Risks

Being a non-deposit taking NBFC most of the adverse movements in interest rates could possibly pose a risk to the ability to raise funds for managing liquidity gaps - giving rise to LIQUIDITY Risks.

As a measure for effectively managing the risk in the company has put in place the risk limits for such exposures. As part of the mitigating plan ALCO monitors the risk for proactive actions.

The Asset Liability Management Committee (ALCO) of the company, at the Management Level and both the Audit Committee of the Board as well as the RISK MANAGEMENT COMMITTEE OF THE BOARD, at the Board Level, will closely monitor any mismatch positions and the macro-environment to consider all indicators of risks, to plan and advise suitable actions.

5.3 Operational Risk

5.3.1. Definitions

Operational Risk originates from failures in internal processes, people, systems, or from external events. Given its pervasive and dynamic nature, Operational Risk is inherent in every product, activity, process, and system of the Company.

While financial institutions traditionally devote significant resources toward managing Credit Risk and Market Risk, experience across jurisdictions has demonstrated that Operational Risk often poses equally significant, and at times greater, threats to financial stability. Operational Risk events can result in substantial financial losses, regulatory penalties, reputational damage, and in severe cases, rapid erosion of net worth and capital.

In several instances globally, Operational Risk events have led to losses exceeding those arising from traditional risk categories, thereby significantly impacting capital adequacy and profitability. The allocation of appropriate levels of capital to cover Operational Risk exposures directly influences the cost of capital and may adversely affect Return on Assets (ROA) and overall business performance. Accordingly, Operational Risk must be dimensioned, monitored, and reviewed with rigor and discipline.

The activities which Company shall undertake expose it to various types of Operational Risks, and hence the company is required to establish a robust Operational Risk management framework. This policy should be framed in line with the Reserve Bank of India (RBI) issued vide DOR.ORG.REC.21/14.10.001/2024-25 an updated "Guidance Note on Operational Risk Management and Operational Resilience" on April 30, 2024. This guidance note is applicable to Non-Banking Financial Companies (NBFCs) and aligns with the Basel Committee on Banking Supervision (BCBS) principles. Or any other guideline that might be in force, from time to time.

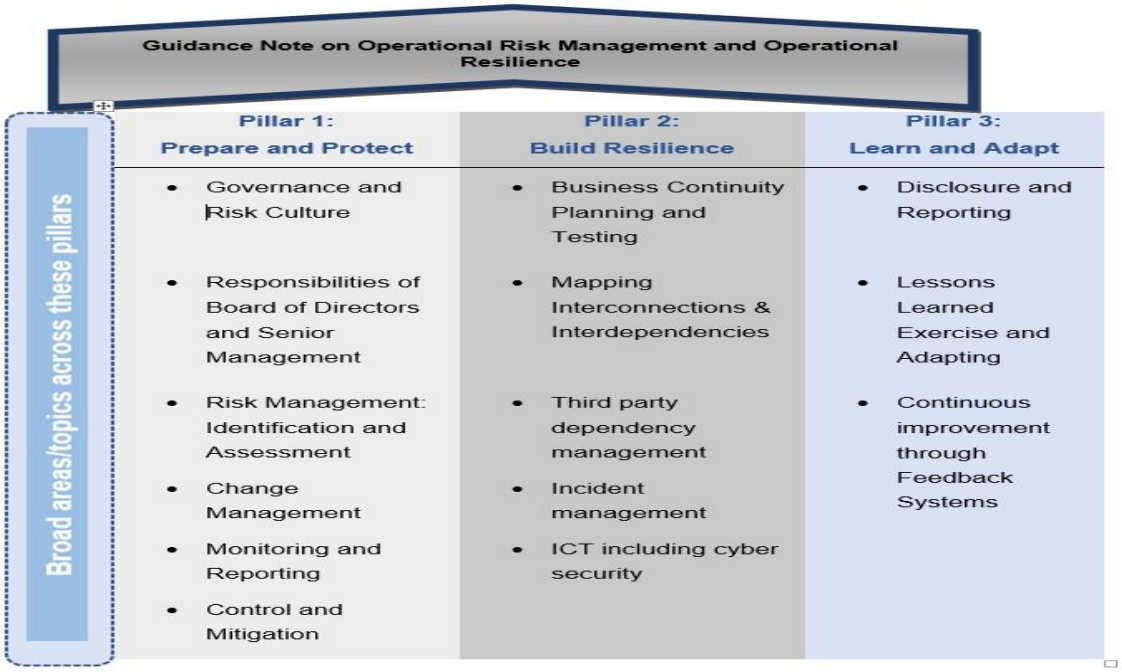
This Guidance Note on Operational Risk Management and Operational Resilience has been built on three pillars.

The three pillars are:

(i) Prepare and Protect

(ii) Build Resilience

(iii) Learn and Adapt



These three pillars support a holistic approach to the management of Operational Risk and Operational Resilience and create a feedback loop that fosters perpetual embedding of lessons learned into the Company's preparation for operational disruptions and its performance during actual occurrences of disruptions.

Companies' business activities across Gold Loans, Vehicle Loans, and MSME Loans expose it to a wide range of Operational Risks, including but not limited to:

- Process failures and control weaknesses
- Human error and employee misconduct
- Fraud and forgery risks
- Information and Communication Technology (ICT) failures
- Cybersecurity threats
- Third-party and outsourcing risks
- Business disruption events
- Compliance Risks.

5.3.2 Operational Risk Management Framework (ORMF)

Operational Risk is a complex risk category when it comes to identification, quantification, and mitigation of risk. It is impacted by numerous factors such as internal business processes,

regulatory landscape, business growth, customer preferences, and even factors external to the organization. It is highly dynamic in nature where new and emerging forces such as breakthrough technologies, data availability, new business models, interaction with third parties, etc., continuously create new demands on Operational Risk Management Framework (ORMF).

The concerned Departments/Business units shall facilitate implementation of processes to support the proactive identification and assessment of the significant Operational Risks inherent in all products, activities, processes and systems.

The concerned Departments/Business units shall also be using various MIS reports for RCSA, KRI and Loss data for reporting to the Risk management department which has been detailed Operational Risk Management Process Manual.

The individual risks under the above broad risk categories and approach & system to deal with the various risks are listed in greater detail in the following paragraphs. In addition, a "Risk Register" listing the various individual risks in granular form will be compiled giving the risk cause, risk impact, risk degree, steps to mitigate the risk and the responsibility points.

5.3.2.1 ORMF Objectives

- Meet or exceed Reserve Bank of India (RBI) and Basel III or any other requirements on Operational Risk Management, from time to time, in the Company.
- Assign clear accountability and responsibility for management and mitigation of Operational Risk
- Develop a common understanding of Operational Risks across the company, to assess exposure with respect to Operational Risks and take appropriate actions
- Strengthen the internal control environment throughout the company reducing the probability and potential impact of Operational Risk losses.
- Minimizing losses and customer dissatisfaction due to failures in processes
- Developing a loss database to collect, record and monitor Operational Risk related losses in the company.
- Compute capital charge for Operational Risk as per the Basel II or any other requirements and RBI guidelines
- Develop techniques for creating incentives to improve the management and mitigation of Operational Risks.

5.3.2.2 Key Elements of ORMF

Operational Risk Management (ORM) governance structure includes Board of Directors and Risk Management Committee and operational heads of functionaries.

ORM Organization Structure: The company's Organizational structure for managing operation risks consists of the following three lines of defense.

- First line of Defense consists of functions that own and manage risk, which in the company consists of all the business units and support functions through adherence to the laid down procedures
- Second Line of Defense consists of functions that oversee risks, which, in company, consists of the Risk Management and Compliance department.
- Third Line of Defense consists of functions that provide independent assurance, provided by Internal Audit, which provides the independent Assurance on the effectiveness of governance, risk management, and internal controls.

ORM Assessment and Measurement Tools: The primary tool for measuring. Operational risk across the Company shall include internal operational loss data. These loss data are used primarily for assessing and monitoring operational risk exposures across the company. RMCB is empowered to modify and implement any additional tools apart from the ones currently in place.

ORM Reporting: Reports on Operational Risk exposures approved by RMCB are used at stipulated frequencies to monitor operational risk exposures within the overall ORMF. Relevant reports will be submitted to relevant forums such as Board, RMCB, business, and support unit heads as described in the respective policy and process documents.

The Risk Report will contain, among other parameters -

i. Overall Risk Rating Dashboard (in RAG Rating standards) with parameters

viz -

a. Financial Parameters

b. CRAR

c. Non-Financial Parameters: Non-IT

d. Non-Financial Parameters: IT Related

ii. Macro/Micro Economic Indicators

iii. Action Plan for RMD till year-end.

RMD Team will approach the concerned departments in the company for the required data to prepare the above report.

5.3.3 Operational Risk Appetite

Company acknowledges that Operational Risk exposure occurs during the normal conduct of business activities.

In order to manage inherent Operational Risks, appropriate tolerance limits, need to be defined. The risk tolerance level should be determined at the business unit/risk level and aggregated up to the legal entity, approved by the RMCB.

Risk tolerance will be reviewed for continuing applicability by both the business areas and/or by CRO on a periodic basis.

The Chief Risk Officer/Head Risk Management, along with the Head of all functional departments (Both Business and non-Business) draw up detailed process documents on how the different Business and Support Units are to arrive at their Tolerance Levels/Limits and also coordinates the periodical activities of setting up of the Tolerance Limits. Based on newly emerging risk areas and the level of risks identified during internal reviews of the concerned departments, the Risk Register, tolerance levels, and limits shall be reviewed and updated periodically, at least once a year. Any modifications or updates identified shall be presented to the next RMCB for approval.

5.3.4 Other Operational Risk Elements

5.3.4.1 Outsourcing of Activities

Non-core functions may be outsourced to reputed and approved agencies that specialize in the activity concerned on the premise that these agencies would perform the tasks more efficiently with or without cost reduction. Some common activities which can be outsourced are document storage, engagement of Direct Sales Agents (DSA), Recovery agents, collection agents etc. Due diligence on the agencies will be ensured. Materiality of Outsourcing contracts will be assessed as per RBI Guidelines and the management of the same will be as prescribed by RBI at all times.

5.3.4.2 Third Party Risk Management (TPRM)

Third Party Risks are key risks as the Company engages with many different external parties for carrying out its activities either on a continuous basis (Outsourcing) or on a contractual basis (consulting assignments, etc.).

These Third-Party Risks have to be managed appropriately at all times to ensure that Company not only realizes the value and objective of the engagement itself but is protected at all times from any extant regulatory and legislative guidelines.

Thus, the Third-Party Risk Management (TPRM) will encompass the Outsourcing Guidelines and the Procurement Practices and will extend to all engagements involving Third Parties, including those parties that may be part of the Group.

Guidelines in the detailed outsourcing policy for financial services and IT outsourcing policy for outsourcing IT related activities approved by the Board and be adhered to by the Company.

5.3.4.3 Business Continuity Management Systems

Businesses can face interruptions at any time, for any reason. These interruptions hamper the ability of the businesses to deliver the committed levels of deliverables to their constituents, particularly its customers.

In today's 24x7x365 world, with increasing growth of the electronic and mobile delivery options (services) and their usages, it is now incumbent on us to ensure that there is a structured approach to manage such interruptions, through proper Business Continuity Management Systems, that include the Business Continuity and Disaster Management Plans and Processes.

The company adopts the guidelines enshrined in the ISO Standard 22301 - the Global standard for Business Continuity Management Systems.

5.3.4.4 Risk-Based Internal Audit (RBIA)

The company adopts the RBIA guidelines of RBI as a part of its Operational Risk Management Framework. RBIA circular DBS.CO.PP.BC.10/11.01.005/2002-03 dated December 27, 2002

RBIA is a methodology that links internal auditing to the company's overall risk management framework.

RBIA allows the internal audit to provide assurance to the Board that risk management processes are managing risks effectively. The essentials of risk-based auditing are widening the coverage, tackling some of the non-traditional areas, and focusing on helping management achieve its objectives. It requires a demonstration of greater knowledge of the business and allows a much broader level of assurance to be given to the Board.

The RBIA Policy framework of the Company would be structured to capture the above objectives and would guide the company in complying with the same.

5.3.4.5 Information Technology Risk

a) General: The Company has been ahead of other similarly placed NBFCs in the adoption of a fully computerized environment for conducting its business operations. The Company will adopt a Comprehensive IT Policy encompassing acceptability of various usages, asset management, applications management, infrastructure management, and IT security. Some of the important risk-related issues in IT are listed hereunder.

b) Disaster Recovery: Data Centre (DC) & Disaster Recovery Centre (DR): The DC is located in Valapad, Thrissur, and the DR is located in Pollachi, Tamil Nadu. The DC and DR will lie in different seismic zones.

c) Switch over to DR - RTO (Recovery Time Objective) / RPO (Recovery Point Objective): In order that the switchover from DC to DR and vice versa is affected quickly and efficiently,

issues relating to time taken for switchover and consequent data loss in transmission will be addressed and defined.

d) Data Transmission / Communication Lines/Power Supply: Redundancy of leased lines/broadband for data transmission is provided at DC, DR and branches also between DC and DR. The adequacy of the bandwidth of the leased line/broadband will be reviewed periodically and upgraded as per need. An uninterruptible power supply (UPS) will be ensured at all offices.

e) Data storage and access: Database server gets updated online. Only authorized personnel will have access to the database. The scope to tamper or alter the database will be eliminated through controls. Access to data/applications will be on a 'need-to-know' basis. Transaction rights will be conferred only on those requiring it by virtue of the nature of their duties.

f) Applications (software): Only authorized and licensed software will be loaded into the system, central and at various user points. The licensing position will be reviewed periodically to guard against violations of IT Copyrights / Laws.

g) IT Security: A secured system of access control, both on-site and remote, including password management and secrecy will be in place and reviewed periodically. Suitable anti-virus 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.

h) Information Security (including Cyber Security): Cyber security strives to ensure the attainment and maintenance of the security properties of the assets of the organization and its users against relevant security risks in the cyber environment. The Cyber Security shall lay down safeguards that the company shall apply to its information resources and assets to mitigate various cybersecurity risks. The company shall implement security controls at all levels to protect the confidentiality, integrity and availability of information during processing, handling, transmission and storage. The company shall endeavor to identify the various resources, including people, processes, tools and technologies, which

can be utilized to prevent, reduce or manage the risk associated with a cyber- incident. All existing policies related to personnel, administration, protection of confidential information, and other relevant areas would apply equally to the information resources.

i) IT Services Management (Helpdesk): An efficient system to report and manage IT incidents and problems will be in place across the network of offices.

j) Responsibility: The overall responsibility for managing and monitoring the IT related risks will lie with the Head of the IT Dept. A suitable 'service level agreement' between IT Dept and Business Units will be defined and implemented.

5.3.4.6 Risks in IT outsourcing

Financial institutions have been extensively outsourcing their IT services requirements to third parties in order to get easier access to newer technologies. This exposes them to

significant financial, operational, and reputational risks. RBI on June 23, 2022 issued.

Draft Master Direction on Outsourcing of IT Services and thereafter, on April 10, 2023, RBI issued the final directions on IT Outsourcing Directions: Master Direction on Outsourcing of Information Technology Services.

Governance Framework - IT Outsourcing Policy:

The company shall put in place a comprehensive Board-approved policy covering

the following key aspects:

- Roles and Responsibilities of the Board, its committees, and Senior Management.
- Criteria for selection of IT activities being outsourced and the service providers, which can also be group entities or cross-border service providers. (Arm's length basis to be followed for arrangements with group entities).
- Engagement of Service Providers: The company shall undertake due diligence before engaging a Service Provider based on a risk-based approach, considering qualitative, quantitative, financial, operational, legal, and reputational factors. Further, wherever possible, it shall also obtain independent reviews and market feedback on the Service Provider to supplement its own assessment. The factors for conducting due diligence includes capability, financial soundness, business reputation, information/ cyber security risk assessment etc.
- Outsourcing Agreement: MAAFIN shall enter into legally binding agreements defining the rights and obligations of each of the service providers.
- Risk Management: The Company shall have a Risk Management Framework that comprehensively deal with processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with outsourcing of IT services arrangements.
- Reporting of Cyber Attacks: It shall be ensured that the cyber incidents are reported to MAAFIN by the service provider without any undue delay, so that it is reported to the RBI within 6 hours of detection by the Service Provider.
- Business Continuity and Disaster Plan: The company shall ensure that its service providers have a robust framework for maintaining and testing the Business Continuity Plan (BCP) and Disaster Recovery Plan. It shall evaluate the possibility of bringing the outsourced activity back in-house in an emergency situation. In the event of an unexpected termination or insolvency/liquidation of the service provider, it shall be ensured that measures are in place for removing all the assets from the possession of the Service Provider.

5.3.4.7 Financial Crime Risk /Counter Terrorist Financing (FC/CTF) Risk

Counter Terrorist Financing (CTF) are laws and regulations aim to stop the illegal financing of terrorism and terrorist-related activities. It is closely tied to anti-money

laundering (AML). The Company has been conducting transaction monitoring, filing of STR and CTR, and KYC / AML risk assessment on a quarterly basis.

- This acts in conjunction with Companies 's Know Your Customer (KYC) and Prevention of Money Laundering Policy.

5. 4 Other Risks (Other than CR/MR/OR)

5.4.1 Regulatory / Compliance Risk

a) General: The Company is an NBFC coming under the regulatory purview of the Reserve Bank of India and the Ministry of Corporate Affairs. In addition, the Company is also required to comply with various central, state, and commercial laws applicable in the conduct of the various activities of the business.

b) Meeting with compliance requirements: The Company recognizes that the regulatory landscape is under periodical review and this requires the Company to be proactively prepared, as best as possible, to meet with the challenges posed by the changes. The Company will respond effectively and competitively to regulatory changes, maintain appropriate relationship with the regulators/ authorities strengthen the reliance on capital and improve the quality of in-house compliance. All reports, returns and disclosures stemming from regulations will be submitted promptly and accurately to reflect the correct position. Business processes will be defined in a manner to ensure comprehensive regulatory compliance considering the multitude of regulatory agencies the Company has to deal with.

c) Responsibility: Competent and knowledgeable specialist officers will be recruited to ensure compliance. The responsibility for ensuring compliance with regulatory requirements and directives on a day-to-day basis will rest with the Business Heads. The Internal Audit Dept of the Company will provide the assurance through the audit of the compliance levels.

5.4.2 Reputational Risk:

a) General: Reputation risk is the loss caused to the Company due to its image or standing being tarnished by certain incidents or actions arising from its business operations. Such incidents or actions may be attributable to the Company or any employee(s) or executive(s) committed either consciously or otherwise. Reputation risk could result in loss of revenues, diminished shareholder value and could even result in bankruptcy in extreme situations. Reputation loss can be caused by mere negative perceptions and could occur even if the Company is actually not at fault. Reputation risk is considered even more threatening to Company value as compared to say credit risk. In fact, good reputation is an intangible asset like goodwill. The Company recognizes that while reputation is built over years it can get blotted in a flash. The Company, therefore, considers protecting its reputation of paramount importance.

b) Causes: Some common examples of actions resulting in fall in reputation are grossly incorrect financial statements, deliberate dishonest actions of employees especially those in senior management, recruitment of persons without proper screening process, frequent

serious and/or large value frauds, window dressing of business position, data security breaches, violation of customer secrecy, dealing with criminals and extending loans for

unlawful activities, poor security arrangements, obsolete system / procedures/practices, dealing with vendors having bad reputation, adopting illegal or unethical business practices, evasion of taxes, charging exorbitant interest rates, dishonoring commitments etc.

c) Mitigation: Risks to the Company's reputation will be addressed by:

- Instituting a strong risk management system, including fraud prevention and creating a culture of risk awareness across the organization.
- A commitment to transparency, morality, and accuracy in operations, including the correctness of financial statements for public use.
- Maintaining a robust and effective communication channel across the organization, including all stakeholders such as Directors, Shareholders, Regulators, Lenders, Customers, Employees, Vendors, etc.
- Encouraging and rewarding ethical behavior amongst employees. Ensuring immediate but fair action against employees indulging in unethical action or behavior.
- Ensuring prompt compliance with regulatory directives and other laws, both in letter and spirit.
- Institutionalizing customer service excellence supplemented with an efficient complaint redressal mechanism.
- Constituting a 'crisis management team to address sudden and unanticipated events.
- Maintaining effective liaison with media and issuing prompt clarifications or rebuttals to negative reports
- The Company shall monitor emerging reputational risk drivers, including customer feedback, media and social media developments, ESG (Environmental, Social and Governance) considerations, and brand perception indicators. Appropriate mechanisms shall be established to identify, assess, and respond to such risks in a timely manner.

d) Responsibility: The responsibility for protecting the reputation of the Company and taking steps to enhance the Company's standing will lie across all functionaries in the organization which will be regularly overseen by the Chief Risk Officer / Head - Risk Management and reviewed by the Top Management.

5.4.3. Existential risks

Existential risk is defined as one that threatens the premature extinction of Earth or Establishments or Data or the permanent and drastic destruction of its potential for desirable future development of the Institution causing Loss or panic.

The 2007 Financial Crisis and the Covid - 19 pandemic necessitated businesses to think of managing the risks of existence. Recent developments in the world, from tensions brewing between India and China to Ukraine - Russia conflict, have further demonstrated the importance of preparing proactively for catastrophes that seem implausible but are probable.

5.4.3.1 Sources of risks

Some examples of factors that can challenge the going concern of an entity to consider are:

- Massive outbreak of Highly contagious/Infectious disease reaching the level of being declared as pandemic (E.g. Covid – 19).
- Massive and wholesale Breakdown of IT Infra, cyber-security attacks, data fraud.
- Political instability, (including a totalitarian regime taking over), social risks such as humanitarian crisis, social unrests, popular movements, riots, terrorism etc.
- Natural disasters in the nature of a catastrophe.
- Pivotal change in government policies regarding matters fundamental to the business.
- Geopolitical conflicts leading to a full-scale war (including use of nuclear arsenal) and subsequent embargo with countries forming a part of the supply chain. This would also involve consideration of disruption of global value chains and barriers to cross border movement of people and goods.
- Large scale Reputational risk events, bad press, loss of confidence brought on by fraud and other moral and ethical fallouts.
- Regulatory, legal or contractual breach of serious nature
- Abrupt obsolescence of product/technology on which the entity predominantly depends.
- Prolongation of recession occasioned by other calamities.
- Extreme movements in business and macro variables.

5.4.3.2 Existential risk management

The existential risk management is aimed to study, anticipate and safeguard against those events (irrespective of the type of events) that are though unlikely to happen but so severe so as to prove fatal to the going concern/continuity of business.

The exercise of existential risk management will involve rigorous scenario and sensitivity analysis, utilizing the advancements in data analytics and artificial intelligence (AI) as well as expert suggestions to simulate stressed circumstances.

5.4.3.3 Illustrative tools for managing existential risks are:

- Rigorous cash flow forecasting incorporating all plausible scenarios. To ensure its robustness and usefulness, the scenario analysis must be sufficiently extensive with many nodes of possibilities at each step.
- Stress testing business and macro variables, like demand for loan products, ability of the customers to service EMIs, collection efficiency, interest rates

and carrying out sensitivity analysis on solvency and liquidity ratios, capital and other metrics detrimental to the survival of the business.

- In addition to preparing internally for contingencies, external risk management tools like – insurance, special situation bonds like catastrophe bonds and other specialized hedging tools like weather derivatives etc. should be used.
- Plans for managing fixed costs during periods of shutdowns must be thought-out. Cash optimization to identify opportunities to decelerate burn rate and preserve liquidity should be planned. The aim is to hibernate and survive in a state of suspended animation by rationalizing contractual cash outflows.
- Portfolio analysis to assess options to accelerate collections and finding new avenues for raising funds in times of stress.

5.4.3.4 Existential risk mitigants

a) In catastrophic situation the existing model assumptions for Expected Credit Loss provisioning, Capital Adequacy etc. would be insufficient as the simulation is based on the historical data which is no more relevant. This necessitates having models specially designed to be of use in times of extraordinary and unprecedented situations with parameters calibrated accordingly.
b) Equally important is the recovery plan and it must be as comprehensive as time and other resources permit. The business resumption phase of the plan must consider various alternate realities of recovery and simulate the recovery.
c) Another layer of preparation in the form of correlation analysis could be used to consider the cascading effect of these scenarios happening simultaneously. This will render complex scenarios comparable. Interdependencies between risks and functions must be studied in some detail to anticipate the speed and extent of inter-functional diffusion and spill-over of risks.
d) An evaluation of crisis management and business continuity plans of third parties which are important for the existence of our business must also be carried out.
e) A trade-off must be struck between costs and benefits of existential risk management. Plans must be scaled depending on the size of the businesses.

Existential risk mitigants

Events	Responses
Infectious disease outbreak.	• Managing the operations of the company with minimal staff with others working remote / home. • Prepare the IT infrastructure facilitating to work from remote centers. • Make use of the digital services for business and collection.

Breakdown of IT Infra, cyber-security attacks,	Standby (DR) locations of the servers to be located deeply away in geographies that can help to hedge the risk including non-seismic zones
Political instability	Resort to shrink operations so as not to expose the company's interest until matters are stabilized.
Pivotal change in regulations and government policies	Senior management committee to immediately to liaise /represent to the Regulators/Government to explain the position and seek alternative models for maintenance.
Location of the company's Head office at Valapad, close to the coastal area and any likelihood of a e tsunami type events repeating with wider impact cannot be altogether ruled out.	• Security department to monitor earthquake and tsunami related warnings from the authorities concerned and make adequate preparations for evacuating staff and preserving records on a war footing. • Though 2004 tsunami and 2018 deluge have not impacted the entire Manappuram coast (the sea facing area of the island from Chettuva to Kottappuram/Azhikode) as it is not as low lying like the southern part of Kerala, still the Company needs to be mindful in monitoring and making preparations. The Company's data center is located in Valapad and Data Recovery Centre is located in Pollachi. In the case of natural calamity, we can continue our IT based business operations without hindrance. However adequate arrangements will be made to back up any data locally saved for restoration. • All the physical assets are covered by insurance including, if available against tsunami kind of risks. • The Company already has a business continuity plan in which natural calamities also factored in.

5.4.3.5 Existential risk governance

Existential risk management programmed demands deeper and higher level of involvement for a response compatible with the event. Responsibility of managing existential risks vests on the CEO of the company. CEO shall address any such events with the following objectives:

- Designing Crisis/Incident Management
- Business Continuity.
- Business Resumption and Disaster Recovery plans

These plans should define the when, who, where and how and a coordinated response will be initiated in the event of crisis. The plans must be dynamic, evolving constantly to adapt to changing environment. They must be regularly tested for effectiveness and communicated across the value chain to ensure that employees are well aware of their roles and responsibilities in case of any eventualities. Institution of robust Business Continuity Management (BCM) shall ensure that the organization recovers significantly quickly during unforeseen events.

5.4.5 External Event Risks

The Company recognizes the external events such as fire, natural calamities, riots, civil commotion, strikes, pandemics, infrastructure disruptions and other force majeure events may materially impact the company's operations, assets, employees, customers and reputation.

Such risks shall be managed under the Operational Risk Framework as part of the Enterprise Risk Management (ERM) Policy.

The Company shall:

Periodically identify and assess exposure to external event risks cross locations and business operations.

Maintain adequate Insurance coverage commensurate with the nature and scale of operations.

Establish clear incident escalation and reporting mechanisms, including regulatory reporting where applicable.

Review risk exposure and mitigation measure periodically through the Risk Management Committee.

5.4.6 Crisis Management Team:

The Company shall constitute a **Crisis Management Team (CMT)** comprising senior officials from key functions such as Risk Management, Operations, Finance, IT, Compliance and Human Resources to respond to and manage crisis situations that may adversely impact the Company's operations, reputation, financial stability or regulatory compliance. The CMT shall be responsible for assessing the nature and severity of the crisis, initiating appropriate response and recovery measures, ensuring business continuity, coordinating internal and external communication, and reporting the developments to the Managing Director/CEO and the Board or its Committees, as appropriate. The team shall also periodically review preparedness measures and ensure alignment with the Company's Business Continuity and Disaster Recovery frameworks.

5.4.4 Residual risks

While it is impossible to eliminate all of an organization's risk exposure, the risk framework helps the organization prioritize which risks it wants to more actively manage. The Company has adopted a Risk Tolerance Policy and Framework wherein the tolerance levels of various risk points are captured. This is a dynamic framework. While the Risk, Compliance and Audit team continually monitor adherence to

various risk points affecting the company, the risk tolerance parameters need to be modified subject to changes in the market and risks being faced by the organization. Senior Management reviews the risk tolerance parameters periodically and suggests new parameters within which risk in the company to be managed.

6. Risk Governance in the Company

The Risk Governance structure for the company will be both at the Board level and at the Management level.

6.1. Key Principles of Risk Governance

The Company's risk governance framework is based on the following key principles:

While the Board of Directors will be responsible for overall governance and oversight of core risk management activities, execution strategy will be delegated to the Risk Management Committee of the Board (RMCB) and further sub-delegated to the following Management Level Risk Committees, namely, the Asset Liability Management Committee (ALCO) & the Central Credit Committee.

Segregation of duties across the 'three lines of defense' model, whereby front office functions, risk management & oversight, and Internal audit roles are played by functions independent of one another. Risk strategy is approved by the Board on an annual basis and is defined based on the company's risk appetite in order to align risk, capital, and performance targets

All major risk classes are managed through focused and specific risk management processes. These risks include credit risk, market risk, operational risk and liquidity risk. As the company gains sophistication in risk management, it shall put in place advanced risk management models commensurate with the size, scale and complexity of its business.

Policies, processes and systems shall be put in place to enable the risk management capability. The Risk department/ function shall have appropriate representation on management committees of the company and its respective businesses to ensure risk view is taken in to consideration in business decisions., monitoring, stress testing tools and escalation processes shall be established to monitor the performance against approved risk appetite.

The Risk Management Committee of the Board (RMCB), Asset Liability Management Committee (ALCO), the Central Credit Committee (CCC), the Outsourcing Committee shall have presence of the Chief Risk Officer at all times.

6.2. Risk Management Committee of the Board (RMCB):

6.2.1. Composition of the RMCB

The RMCB is the body responsible for the management of Risks in the company and it manages the same through oversight of the risk management function of the Company, and through approval of the various policies and processes of the Company.
The composition of the RMCB shall be as under:

- The RMCB shall comprise three directors of the Board
- The Chief Risk Officer will be a permanent invitee along with the CFO & CEO
- The Company Secretary shall be the Secretary of the RMCB.
- RMCB shall always be chaired by an independent director of the Board.
- The Chairman and members of the RMCB will be approved by the Board of
- Directors.
- The quorum for a meeting of the Risk Management Committee shall be two members

6.2.2. Frequency of Meeting

The RMCB shall meet once in a quarter - and at least 4 times in a financial year. The meetings of the risk management committee shall be conducted in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

6.2.3. Roles and Responsibilities of the RMCB

The key responsibilities of the Risk Management Committee of the Board (RMCB) include:

1. Approve/recommend to the Board for its approval/review of the policies, strategies and associated frameworks for the management of risk
2. Approve the risk appetite and any revisions to it
3. Sub-delegate its powers and discretions to executives of the company, with or without power to delegate further.
4. Ensure appropriate risk organizational structure with authority and responsibility clearly defined, adequate staffing, and the independence of Risk Management functions
5. Provide appropriate and prompt reporting to the Board of Directors in order to fulfil the oversight responsibilities of the Board of Directors
6. Review reports from management concerning the company's risk management framework (i.e. principles, policies, strategies, process and controls) and also discretions conferred on executive management, in order to oversee the effectiveness of them.

7. Review reports from management concerning changes in the factors relevant to the company's projected strategy, business performance or capital adequacy
8. Review reports from management concerning implications of new and emerging risks, legislative or regulatory initiatives and changes, organizational change and major initiatives, in order to monitor them.
9. Ensure adherence of the extant internal policy guidelines and also regulatory guidelines.
10. Review performance and set objectives for the company's Chief Risk Officer / Head Risk Management and ensure he/she has unfettered access to the Board.
11. Oversee statutory / regulatory reporting requirements related to risk management
12. Monitor and review capital adequacy computation with an understanding of methodology systems and data
13. Approve the C testing results / analysis and monitor the action plans and corrective measures periodically.
14. Monitor and review of non-compliance, limit breaches, audit / regulatory findings, and policy exceptions with respect to risk management
15. The RMCB will be responsible for reviewing and confirming order/decisions of identification of willful defaulters given by the Central Credit Committee.
16. Formulate a detailed risk management policy which shall include:
    (a) A framework for identification of internal and external risks specifically faced by the company, in particular including financial, operational, sectoral, sustainability (particularly, Environmental Sustainability and Governance (ESG) related risks), information, cyber security risks or any other risk as may be determined by the Committee.
    (b) Measures for risk mitigation including systems and processes for internal control of identified risks.
    (c) Business Continuity Plan.

17. Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
18. Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
19. Periodically review the risk management policy, once in a year, including by considering the changing industry dynamics and evolving complexity.

20. Keep the Board of Directors informed about the nature and content of its discussions, recommendations and actions to be taken.
21. The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the RMCB.

The RMCB shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board of Directors.

The RMCB shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

6.3. Management Risk Management Committees (MRMC)

The Company will have a distinct and separate MRMC for each of its key aspects of risks as follows:

1. MARKET & LIQUIDITY Risks: ALCO (Asset Liability Management Committee)

The CRO/Head of Risk Management will prepare the Charter for each of these MRMCs and the MD is authorized to review and approve the charters

6.3.1. Composition of the MRMCs:

Sl. No	Name of Committee	Members of the Committee
1	ALCO – Asset Liability Management Committee	1. MD – Chairman 2. CEO 3. Chief Financial Officer 4. Chief Risk Officer 5. Chief Compliance Officer Head – Treasury / Funds Management (Secretary to ALCO)
2	CCC-Central Credit Committee	1.CEO 2.CFO 3.CRO (Head of Business Concerned will be Secretary of CCC)
3	Outsourcing Committee	1) MD 2) CEO 3) CFO 4) CS 5) GM & CRO

		6) GM & CCO 7) CISO- Special invitee Asst at the Compliance dept shall be the secretary

6.3.2 Asset- Liability Management Committee (ALCO): The ALCO, consisting of the company's top management, shall be responsible for implementing its liquidity risk management strategy.

Responsibilities of ALCO: ALCO would also be responsible for ensuring adherence of liquidity risk limits set by the Board as well as deciding business strategies of the company in line with the overall budget and risk management policy and shall review/decide the following:

- Review of Liquidity Mismatches.
- Review of Interest-Rate Sensitivity position.
- Review of Resource Raising and Deployment vis-a-vis Cost of borrowings/ Yields on advances.
- Review the product mix and product pricing.
- Strategies for deployment of surplus funds.
- Decision on Entering into interest rate derivatives contracts.
- Decision on hedging currency risk.
- Concentration of funding.
- Availability of unencumbered assets.
- Review movements in book to equity ratio, Price to Book value, market price etc., Review coupon at which long term and short-term debts are raised vis a vis the peers.
- Review of LCR requirements and maintenance of HQLAS (High Quality Liquid Assets).
- Review of any other directions from RBI relating to ALCO functions.

The role of the ALCO with respect to liquidity risk shall also include, inter alia, decisions on desired maturity profile and mix of incremental assets and liabilities, sale of assets as a source of funding, the structure, responsibilities, and controls for managing liquidity risk, and overseeing the liquidity positions of all branches.

Quorum of ALCO: One-third of the total members or three members, whichever is higher, will constitute the quorum.

Periodicity of Meeting and Discussion Points: The CFO will arrange for convening the meetings of ALCO once in a quarter or as and when needed depending upon the necessity. Minutes of the meeting shall contain discussions in detail and shall be placed to the Board for noting.

The following areas of liquidity risks (Illustrative) should be deliberated by ALCO

- Compliance with liquidity risk tolerance levels
- Liquidity cost, benefits, and risks in internal pricing
- Off-balance sheet exposures and contingent liabilities
- Funding and capital planning
- Collateral position management
- Profit planning and growth projection
- Forecasting and analyzing 'What if ' scenarios and preparation of contingency plans.
- Interest rate sensitivity

6.3.3 Central Credit Committee (CCC)

- Setting Tolerance limits for each of the parameters included in the Risk Tolerance Policy
- Suggesting improvements to be brought in the credit appraisal methods
- Suggesting and recommending any new credit engines to be procured for improving credit underwriting process/standards
- Suggesting changes to be brought in the credit policy for improving credit quality/business.
- Evaluation of high value credit proposals of Rs 20.00 lakhs & above for credit worthiness.

Quorum of CCC: CEO/CFO, CRO & the Head, Business shall constitute the quorum.

Periodicity of Meeting and Discussion Points: The Head, Business Unit will arrange for convening the meetings of CCC once in a quarter or as and when needed, depending upon the necessity. Minutes of the meeting shall contain discussions in detail and shall be placed to the Board for noting.

6.3.4 Outsourcing Committee

The Committee shall be responsible for reviewing all the outsourcing arrangements, the Company has entered in to, so as to ensure that the outsourcing arrangements the Company have, are in compliance with the Master Directions on Outsourcing issued by the RBI, from time to time.

Responsibilities of the Outsourcing Committee

- Review of all outsourcing arrangements, as per the periodicity stipulated by the RBI
- To evaluate the risks involved in the outsourcing arrangements
- To review the audit reports of outsourcing arrangements
- To ensure that all the outsourcing arrangements are in line with the Master Directions issued by the RBI, from time to time.

Quorum for the meeting will be four- MD/CEO and the other three members.

Note: The Company follows the practice of reviewing operations and Credit risks in Periodic Review meetings (PRM). As operational risks in the company are not complex, and review by PRM is sufficient to identify and mitigate operational risks, formation of CORG may be kept in abeyance.

6.4. Frequency of Meetings of MRMCs:

All MRMCs will meet as per periodicity and submit their reports, including MOM, to the RMCB, through the CRO, for review at its next quarterly meeting.

7. Management Structure of Risk Management in MAAFIN

RISK MANAGEMENT

MAAFIN Adopts the "3 LINES OF DEFENSE MODEL" for the management of its Risks.

- The 1st Line Defense shall always be the Business and Support Units that will own the risks and manage the same, as per the laid down Risk Management Guidelines.
- The 2nd Line of Defense will always be the Risk Management Department, the compliance Department that would support the 1st line of Defense by drawing up of suitable risk Management guidelines from time to time to be able to manage the risks of the company.
- The 3rd Line of Defense will always be the Audit Functions-Primarily the internal Audit Functions that are supported by the external Audits-and other audits like Regulatory Audits, etc. The 3rd line of defense focuses on providing the assurance that risk management principles/policies and process are achieving the objectives of management the risks of the organization at all times.

  The primary responsibility for managing risks on a day-to-day basis will continue to lie with the respective business units of the company.

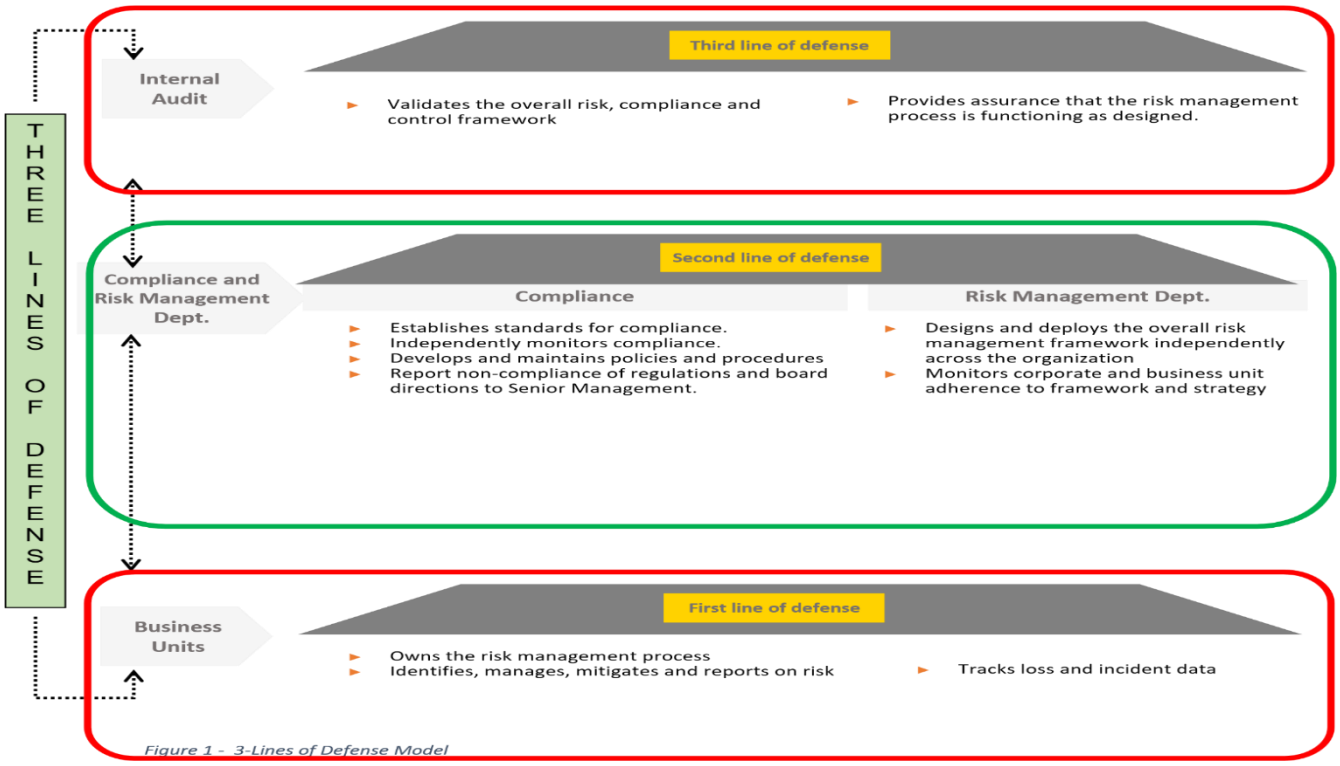


Figure 1 - 3-Lines of Defense Model

7.1 Role and Responsibilities of the Risk Management Department (RMD):

The broad responsibilities of the RMD are:

i) Implementing the Risk Management Policy as approved by the Board of Directors. Reviewing the provisions of the policy periodically and recommending to the Board of Directors appropriate modifications or improvements if required.

ii) Championing the cause of risk management and instilling a culture of risk awareness across the length and breadth of the organization.

iii) Identifying the various risk points in the organization and assessing or measuring their impact on the business.

iv) Devising proactive and reactive strategies for controls and mitigation of risks.

v) Designing or assist in the designing of work processes or activities

having risk implications, getting them approved, assisting in implementation of the processes and engaging in periodical review of the effectiveness of such processes.

vi) Development of 'models' for assessment of loss in projected circumstances.

vii) Preparing reports to Top Management, Audit Committee and Board of Directors on risk matters.

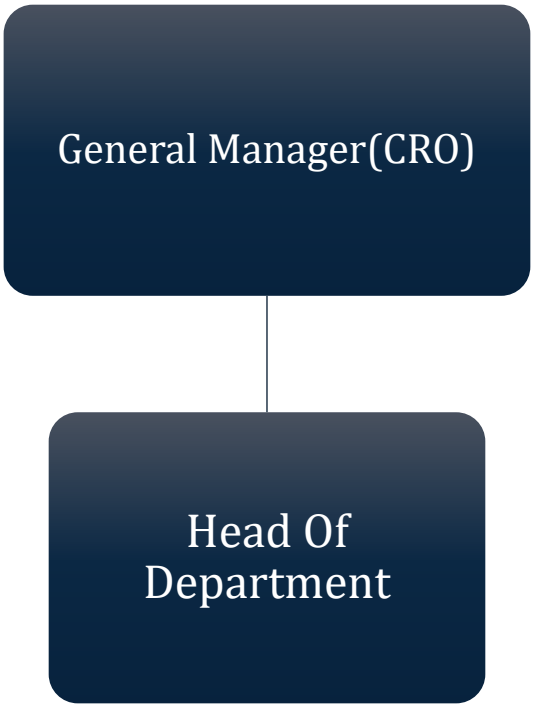
viii) Appraising uncovered / residual risks to the Management / Board.

7.2 The Risk Management Department

The RMD of the company will be an advisory guide for all risk-related matters to all business and support units in the company. This role is more of a "strategic think-tank" and will evolve as the company forays into businesses other than its non-core areas.

The RMD will also set up the 'Conventional' Risk Management processes and help the various businesses and functions to adopt the risk management practices as may be applicable to their businesses and functions, to adopt and embed the same into their day-to-day routine – and continue to monitor the same from a central perspective, while continuing to provide guidance from a "subject matter expert" role

7.3 The Organization Chart of the Risk Management Department



7.4 Roles and responsibilities of CRO

- Identification of risk points in the organization and assessing or measuring their impact on the business.
- Formulation of Risk Management Policies.
- Devising strategies for controls and mitigation of risks.
- Reports to Top Management, Risk Management Committee and Board of Directors on risk matters.
- Vetting of product policies from a risk angle.
- Vetting credit proposals from a risk angle.
- Assisting Credit units to develop Credit Assessment Models.
- Conduct portfolio analysis to measure migration in risk.
- Risk vetting of operational guidelines.
- Part of credit approval process.

Member in ALCO, CCC and Outsourcing committees

Assist in setting tolerance limits for various risk parameters

8. Risk Reporting

Enterprise Risk Management will not be completed without a structured process for reporting of risk related information, to all its stakeholders.

Risk Reporting therefore has two significant categories – Reporting to External Stakeholders and Reporting to Internal Stakeholders.

8.1. Risk Reporting to External Stakeholders:

External Stakeholders are always regulatory and legislative bodies. As a Financial Institution, that too one classified as a "Systemically Important" (SI) one, we have many a report to submit on risk related information – mainly from the Credit Risk side, but on the whole, these reporting cover an all-round perspective of risks of the Company.

The Compliance Department will not only interact with the Regulators, it will advise all internal stakeholders on the relevant and extant reporting to be followed, from time to time.

8.2. Risk Reporting to Internal Stakeholders

Internal stakeholders are primarily

1. Board of Directors
2. Committees of the Board
3. Top Management Team
4. Functional Management Teams
5. Operational Stakeholders in all SBUs/Support Units

Thus, Risk Reports to Internal stakeholders can be classified as

- Strategic Reports on Risks – i.e. Reports that help formulate or review strategies
- Tactical Reports on Risks – i.e. Reports that help review the need for course corrections
- Functional Reports on Risks – i.e. Reports that help measure the risk-metrics in a structured and consistent manner across all functional units of the company, and those that become the basic source of any MIS reports on Risks of the Company.

8.3.1 Reporting to the Managing Director & the Board of Directors on Risks

8.3.1.1. Risk Adjusted Return on Capital (RAROC)

Risk-adjusted return on capital (RAROC) is a risk-based profitability measurement framework for analyzing risk-adjusted financial performance and providing a

consistent view of profitability across businesses. The concept was developed by Bankers Trust and principal designer Dan Borge in the late 1970s.

Under our revised Risk Management Model, the Company now adopts the RAROC as the standard measure for decisions on business strategies.

The CRO and the CFO will be responsible for drawing up the necessary changes in the processes that lead to the compilation and use of the data, for the calculation of RAROC.

8.3.1.2 Periodic Reporting to RMCB

The CRO will submit a detailed summary on the overall Risk Status of the Company, based on the ERM Framework.

This status report will be in the form of a dash-board, with relevant details.

9. Others

9.1 Independent risk function: CRO shall not be assigned any business targets nor shall they be engaged in regular business functions of the company. CRO shall report to MD. The Board / Risk Management Committee shall discuss with CRO on the risks in the company without the presence of MD&CEO once a quarter.

9.2. Inter–relationship among authorities exercising control functions: The risk management function, compliance function, vigilance function and internal audit function together form a coherent whole of transversal control functions between which coordination is required. These control functions shall be harmonized and ensure sufficient sharing of relevant information among them. During the periodical review of each department, representatives of other department should be present as invitees for seamless sharing of information.

The Policy shall be reviewed by the Risk Management Committee of the Board and put up for approval by the Board of Directors annually or in the event of major changes in the Risk Management Processes. Exigencies, if any, shall be reported and approved by the Board of Directors through the RMCB at the next possible meeting. The functions and tools of the Risk Management Department shall be reviewed atleast annually and any gaps identified shall be placed before the Risk Management of Board along with the Recommendations for appropriate modifications, which shall be incorporated during the policy review.

****