MANAPPURAM ASSET FINANCE LIMITED

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	ERM Policy & Framework	27-02-2025

Effective Date	**01/03/2025**
Next Review Date	**Annual review**
Policy Owner	**Risk Management Department**
Prepared By	**Risk Management Department**
Reviewed by	**Policy Review Committee**
Approved By	**Board**

Contents

1. 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, Two Wheeler Loans and Micro Finance Loans

The current policy is renewal of the existing policy framework, incorporating relevant portions of the 'Draft Guidance Note on Credit Risk Management' published by the RBI on 07/08/2024 and the 'Guidance Note on Operational Risk Management and operational resilience 'published by the RBI vide DOR:ORG:REC 21/14.10.001/2024-25 dated 30/04/2024 and also by incorporating more features like reputation risk management, liquidity risk management etc.

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."

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 appraised 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 growth with profitability within the limits of risk absorption capacity. It is expected to facilitate the Company acquire and maintain a pre-eminent position amongst NBFCs.

3. Risk Management Approach: The Repositioned Approach

The vision envisaged by the thinking of the entire Board of Directors – to reposition the risk management approaches and take it to the higher level of "strategic think-tank" of the Company, will be the driver of the repositioned approach to Risk Management in the company.

However, it is also recognized that the "conventional" approach of 'structured risk management practices' would be bedrock on which the higher-level approaches can function effectively. The 'structured risk management practices' would eventually be donned at the functional/business practices, as embedded parts of their own processes, in regular day to day functioning of the company, with the Risk Management function playing the role of an "Advisory Consultant"

As such, and to sum up, the company is not envisaging the jettisoning of the standard and structured risk management approaches but is looking to build a new-generation approach to risk management practices.

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. Micro Economic 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.

The company has a 4th Category called "Other Risks" which typically includes those not categorized into the above 3 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

'C*redit risk model'* refers to any quantitative method that applies statistical, economic, financial, or mathematical principles and assumptions to process data into an output to be used for credit decisions.

Credit decisions, for the above purpose, shall cover all decisions involved in management of a credit exposure and may *inter alia* include credit scoring and borrower selection; pricing of loans; risk analysis of various loan categories; estimating loan loss provisions and economic capital.

5.1.1.1 Introduction & Scope of the Policy

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.

5.1.1.2 Objective

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

i. Establish a governance framework to ensure an effective oversight, segregation of duties, monitoring and management of credit risk in the company.
ii. Lay down guiding principles for setting up & monitoring of the credit risk appetite & limits.
iii. Establish standards for 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.

5.1.1.3 Policy Administration Process

The Risk Management Policy represents the minimum standards for credit risk management and is not a substitute for experience, common sense and good judgment.

Given that the Risk Management Policy is to be flexible and responsive to changing market and regulatory conditions, it will be reviewed by the Chief Risk Officer(CRO), from time to time and any revisions will be updated annually or as necessary. In the event that clarification on interpretation is required, consultation must first be sought from the Risk function.

A. <u>Governance and oversight</u>

- There shall be governance and over sight with regard to model risk management framework for all models deployed, covering the entire model life cycle. The frame work shall cover, *inter alia*, details of governance and oversight aspects commensurate with model materiality; processes around model development or selection; documentation for models deployed; independent vetting / ongoing validation or review processes; change control; and the monitoring and reporting framework including role of internal audit function. The frame work shall also cover the approach with regard to adoption and usage of third-party models. The Company shall maintain a Model Inventory of approved models, insourced or outsourced, with critical information on it.
- The deployment of individual credit models adopted under the frame work and any subsequent changes in their

inputs or assumptions, shall be with the approval of the Risk Management Committee of the Board (RMCB)

B. <u>Model development and deployment</u>

- The models used by the Company may either be developed internally or sourced from external third-party suppliers, including under collaborative lending arrangements, or can be a mix of both as per the provisions of the policy, subject to the following broad principles:

  a. The objectives of the model, problem statements and solution sought from the model should be clearly defined and shall be essential pillars of model development.

  b. The inputs and assumptions considered for the model development shall ensure adequate robustness, with a view to effectively address the intended objectives of the model on a consistent basis.

  c. There shall be a detailed documentation for each of the models which should include the details of the sensitivity of the outputs to the assumptions and inputs, to facilitate clear understanding by the company users, its top management and supervisors.

  d. The model should have the necessary scalability and flexibility to meet the needs of dynamic business conditions.

  e. The model shall have the necessary interface with core banking/financial system, liquidity management, asset liability management (ALM) or any other risk management system of the Company .

  f. Outcomes of the model shall be consistent, unbiased, explainable and verifiable. The same shall form part of the model validation framework.

  g. In case subjective factors are used to override model outcomes, then the same shall be as per the provisions of the policy and such deviations shall be suitably documented in an auditable format.

- In case where outsourced/ third party models are used, the models shall *mutatis mutandis* be subject to above broad principles. The contractual agreements with the third parties shall provide for access by the Company to minimum technical documentation on the models being used or acquired that should give reasonable understanding on design, configuration and operation of the model. The Company shall be ultimately responsible and accountable for the integrity and outcomes of outsourced models.

C. Model validation framework

- There shall be a model vetting / validation process, independent of model development / selection, for assessing the robustness of models developed in house or otherwise. Each model shall be validated before deployment as well as after any subsequent amendments owing to material events or as part of periodic reviews, which shall be at least on a yearly basis. The Company may also consider engaging external experts for validation of the models deployed by them, as provided under their policies.
- The validation exercise shall *inter alia* include review of assumptions underlying the model for their validity / substantiation verification of the accuracy of data used in the model and reliability of data sources; confirming compliance with extant regulatory / statutory instructions; evaluation of model documentation for completeness and accuracy, and assessment of the efficacy of the model outcomes through back-testing. Besides, the validation exercise shall comprehensively review all the limitations and weaknesses in the models, including instances of bias or discrimination, if any, to ascertain the need for suitable corrective measures.
- Validation outcomes shall, *inter alia*, be in terms of suitable and easily understood *ex ante* parameters. The results should be compared against benchmarks prescribed in the policy framework and should be placed before the Risk Management Committee of the Board (RMCB) or the designated Sub-Committee of the Board as mentioned at clause B above.
- The models deployed by the Company shall be subjected to supervisory review. The Reserve Bank may also engage external experts to validate the models deployed by Company, including the external models deployed for their credit management, based on supervisory risk perception. Accordingly, wherever the Company have engaged external models in terms of clause C above, such arrangements shall include appropriate contractual provisions enabling supervisory evaluation of such models either directly by the Reserve Bank officials or by other external experts as engaged by the Reserve Bank.
- The deployment of individual credit models adopted under the policy, and any subsequent changes in their inputs or assumptions, shall be with the approval of the Risk Management Committee of the Board (RMCB).

5.1.2 Current 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 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

This will at all times have a well-structured Risk Management Policy and Procedure that is duly supported by the Top Management and approved by the Board of Directors.

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 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 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 2 to 10 years, price rate risk is relatively low, unless some fraudulent and malfeasant transactions are occurred..

5.3 Liquidity Risks

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. The Company should have a detailed Liquidity Risk Management Frame work (that would be available with a few restricted users) to be able to address any adverse situation on Liquidity position of the company

5.3.3 Responsibility

The Asset Liability Management Committee (ALCO) of the company– at the Management Level and BOTH 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.

The CFO and the CRO are jointly responsible for managing these risks and will report to the respective committees of the Board on the risk status arising as above.

5.4 Operational Risk

1.Background

1.1 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).

1.2 While Operational Risk Management allows the Company to better identify, assess and mitigate the Operational Risks, Operational Resilience provides it the ability to deliver critical functions in the event of any disruption. Although Operational Risk Management and Operational Resilience address different goals, they are closely interconnected. An effective Operational Risk Management system and a robust level of Operational Resilience work together to reduce the frequency and the impact of Operational Risk events. In view of the above, the policy intends to promote Operational Risk Management and enhance the Operational Resilience of the Company.

5.4.2.Definitions

1. "Business unit" is responsible for identifying and managing the risks inherent in the products, services, activities, processes and systems for which it is accountable and includes all associated support, corporate and/or shared service functions, e.g., Finance, Human Resources, and Operations and Technology. It does not include Risk Management and Internal Audit functions unless otherwise specifically indicated**.**

2 "**Critical operations**" refers to critical functions[1], activities, processes, services and their relevant supporting assets[2] the disruption of which would be material to the continued operation of the Company or its role in the financial system. Whether a particular operation is "critical" depends on the nature of the Company and its role in the financial system. Company's tolerance for disruption should be applied at the critical operations level.

3 "Event management" is the process of identification, analysis, end-to-end management and reporting of an operational risk event that follows a pre determined set of protocols.

4 "**Incidents**" are current or past disruptive events the occurrence of which would have an adverse effect on critical operations of the Company. Incident management is the process of identifying, analysing, rectifying and learning from an incident (including a cyber incident) and preventing recurrences or mitigating the severity thereof. The goal of incident management is to limit the disruption and restore critical operations in line with the Company's risk tolerance for disruption.

5 "**Information and Communication Technology**"[3] refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environment.

6 "**Mapping**" is the process of identifying, documenting, and understanding the chain of activities involved in delivering critical operations. It incorporates the identification of all inter dependencies and interconnections including people, processes, technology and third parties.

7 "**Operational resilience**" means the ability of the Company to deliver critical operations through disruption. This ability enables the Company to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, the Company should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption or impact tolerance.

8 "**Operational Risk"** means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. It includes legal risk but excludes strategic and reputational risk and it is inherent in all banking/ financial products, activities, processes and systems.

9 "**Operational Risk Management"** Operational Risk Management refers to entire gamut of activities right from risk identification, measurement and assessment, monitoring and control, mitigation, reporting to senior management and the Board of Directors on the Company's risk exposures, Business Continuity Management, and learning through feedback for improvement.

10 "Operational Risk profiles" describe the Operational Risk exposures and control environment assessments of business units of the Company's and it considers the range of potential impacts that could arise from estimates of expected to plausible severe losses.

11 "**Respective functions**" refers to the appropriate function(s) within the Company's three lines of defence, which are (i) business unit management; (ii) an independent Operational Risk Management including Compliance function; and (iii) audit function.

12 "**Risk appetite**" is the aggregate level and types of risk,the Company is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.[4]

13 "Risk tolerance" is the variation around the prescribed risk appetite that the Company is willing to tolerate.

14 "Supervisory Authority" means,

Reserve Bank of India in case of Commercial Banks (including Local Area Banks, Payments Banks, Small Finance Banks, and Primary Urban Co-operative Banks), Non-Banking Financial Companies, and All India Financial Institutions.

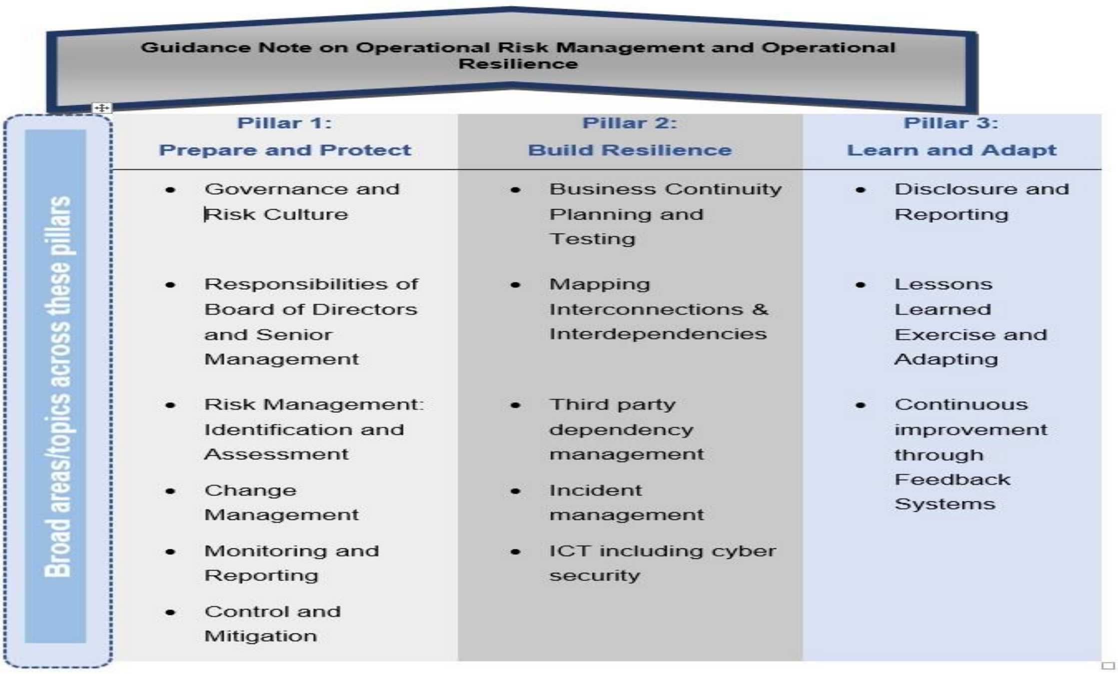
15 "Tolerance for disruption or Impact Tolerance" is the level of disruption from any type of Operational Risk the Company is willing to accept given a range of severe but plausible scenarios.

Resilience has been built on three pillars. The three pillars are:

(i) Prepare and Protect

(ii) Build Resilience

(iii) Learn and Adapt

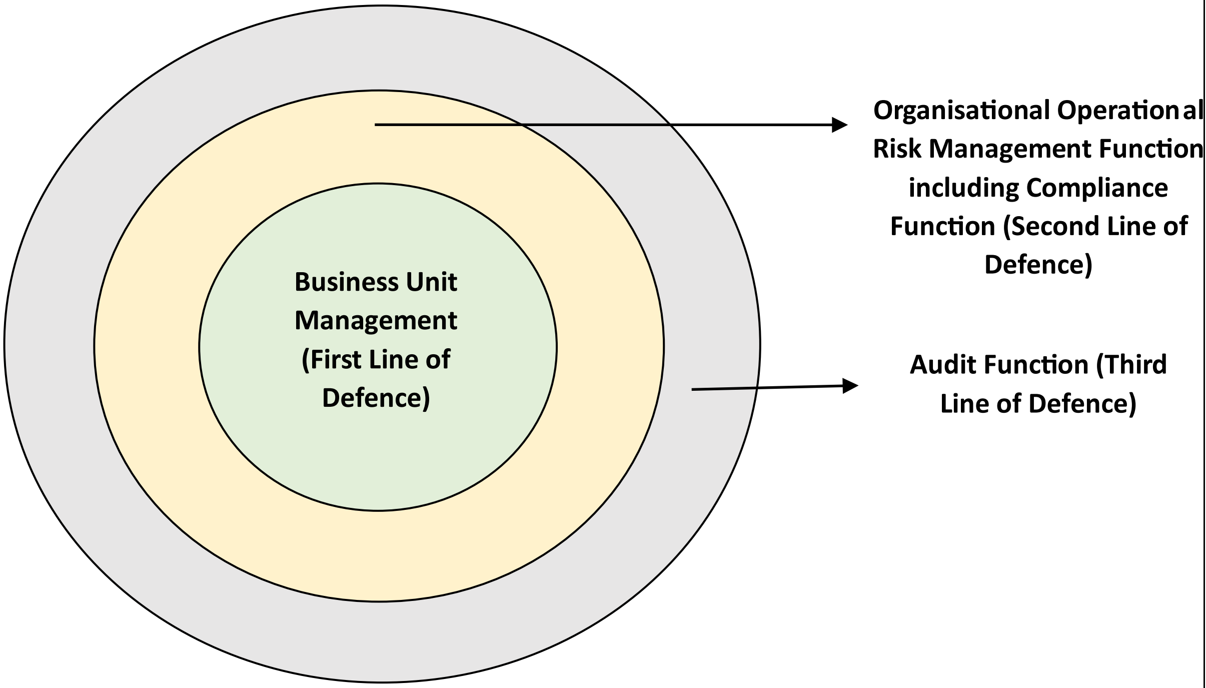


These three pillars support a holistic approach to the management of Operational Risk and Operational Resilience and create a feedback loop that fosters perpetual embedding of lessons learned into the Company's preparation for operational disruptions and its performance during actual occurrence of disruptions.

5.5 Three lines of defence for management of Operational Risk

Sound internal governance forms the foundation of an effective ORMF. The Operational Risk governance function of the Company should be fully integrated into their overall risk management governance structure. Company may leverage its existing risk management functions for this purpose.

As a part of their ORMF, the Company shall rely on three lines of defence:



5.5.1 First line of Defence

Business Unit Management typically forms the first line of defence. Sound Operational Risk governance recognises that business unit management is responsible for identifying and managing the risks inherent in the products, services, activities, processes and systems for which it is accountable. The Company should have a policy that defines clear roles and responsibilities of relevant business units. The responsibilities of an effective first line of defence in promoting a sound Operational Risk Management culture should include:

(i) Identifying and assessing the materiality of Operational Risks inherent in their respective business units through the use of Operational Risk Management tools;

(ii) Establishing appropriate controls to mitigate inherent Operational Risks, and assessing the design and effectiveness of these controls through the use of the Operational Risk Management tools;

(iii) Reporting whether the business units lack adequate resources, tools and training to ensure identification and assessment of Operational Risks;

(iv) Monitoring and reporting the business units' Operational Risk profiles, and ensuring their adherence to the established Operational Risk appetite and tolerance statement; and

(v) Reporting residual Operational Risks not mitigated by controls, including operational loss events, control deficiencies, process inadequacies, and noncompliance with Operational Risk tolerances.

5.5.2 Second line of defence

A Functionally independent Organisational Operational Risk Management Function (OORF) forms the second line of defence. The responsibilities of an effective second line of defence in promoting a sound Operational Risk Management culture should include:

(i) Developing an independent view regarding business units' (a) identified material Operational Risks, (b) design and effectiveness of key controls, and (c) risk tolerance;

(ii) Challenging the relevance and consistency of the business unit's implementation of the Operational Risk Management tools, measurement activities and reporting systems, and providing evidence of this effective challenge;

(iii) Developing and maintaining Operational Risk Management and measurement policies, standards and guidelines;

(iv) Reviewing and contributing to the monitoring and reporting of the Operational Risk profile; and

(v) Designing and providing Operational Risk training and instilling risk awareness.

5.5.3 Third line of defence

The third line of defence, i.e the audit function provides an independent assurance to the Board regarding the appropriateness of Company 's ORMF. This function's staff should not be involved in the development, implementation and operation of Operational Risk Management processes which has been carried out by the other two lines of defence. The third line of defence reviews are generally carried out by Company's internal and/or external audit but may also involve suitably qualified independent third parties. The scope and frequency of reviews should not only be sufficient to cover all activities and legal entities of an Company, aligned with the Company's Operational Risk profile, and identify and prioritize key risk areas that warrant thorough examination but also be responsive to the dynamic nature of the Operational Risk environment. An effective independent review includes two processes

Validation

Ensuring that the quantification systems used by the Company are sufficiently robust as (i) they provide assurance about the integrity of inputs, assumptions, processes and methodologies and (ii) results in assessment of Operational Risk that credibly reflects the Operational Risk profile of the Company ;

Verification

(i) Review of the design and implementation of the Operational Risk Management systems (including compliance and consistency with Board policies) and associated governance processes through the first and second lines of defence
(including the independence of the second line of defence)

(ii) Review of validation processes to ensure they are independent and implemented in a manner consistent with established the company policies;

(iii) Ensuring that business units' management promptly, accurately and adequately responds to the issues raised, and regularly reports to the Board of Directors

(iv) Identifying gaps, if any, in the ORMF and reporting to the Board
and

(v) Providing opinion on the overall adequacy and appropriateness of the ORMF and the associated governance processes across the Company by assessing whether the ORMF meets organizational needs and expectations (such as in respect of the risk appetite and tolerance, and adjustment of the framework to changing circumstances) and complies with statutory and legislative provisions, contractual arrangements, internal rules and ethical conduct.

It is to be ensured that each line of defence:

- has clearly defined roles and responsibilities;
- is adequately resourced in terms of budget, tools and staff;
- is continuously and adequately trained;
- promotes a sound operational risk management culture across the organisation;
- and communicates with the other lines of defence to reinforce the ORMF.

The seamless collaboration between these lines of defence can form a formidable shield, safeguarding not only individual Company,but the entire financial system against potential threats and vulnerabilities.

Some examples of Operational Risks are as follows:

- **Employment Behaviour / Conduct:** Employee Frauds / High Attritions.
- **Infrastructure Related**: Security Breaches leading to Theft / Damage to Physical Assets.
- **Information Security**: Data Leakages.
- **Information Technology**: System Down / Access Controls / Capacity failures.
- **Vendor Management**: Non-Performance / Un Trained Personnel / SLA shortfalls.
- **Compliance Risks**: Regulatory / Legal / Internal Guidelines.

The Risk Management Department (RMD) will 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 RMD will also be using various MIS reports for Risk Control Self-Assessment (RCSA), Key Risk Indicators (KRI), Near Miss Event and Loss data for reporting to the Board

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.

5.6 ORMF – Objectives

The Risk Management Policy aims at the following:

- Meet or exceed Reserve Bank of India (RBI) and Basel II 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

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.

ORM Reporting: Reports on Operational Risk exposures approved by the board 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, 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 (Capital Risk Adequacy Ratio)
c. Non-Financial Parameters: Non-IT
d. Non-Financial Parameters: IT Related
e. Macro/Micro Economic Indicators

ii. 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.

5.6.1 Operational Risk Appetite

It is to be acknowledged 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 Board

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 will draw up a detailed process document on how the different Business and Support Units are to arrive at their Tolerance Levels/Limits and also coordinate the periodical activities of setting up of the Tolerance Limits and Review of the same from time to time.

6 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:

i. Instituting a strong risk management system including fraud prevention and creating a culture of risk awareness across the organization.
ii. A commitment to transparency, morality and accuracy in operations including the correctness of financial statements for public use.
iii. Maintaining a robust and effective communication channel across the organization including all stakeholders such as Directors, Shareholders, Regulators, Lenders, Customers, Employees, Vendors etc.
iv. Encouraging and rewarding ethical behaviour amongst employees. Ensuring immediate but fair action against employees indulging in unethical action or behaviour.
v. Ensuring prompt compliance with regulatory directives and other laws both in letter and spirit.

vi. Institutionalizing customer service excellence supplemented with an efficient complaint redressal mechanism.
vii. Constituting a 'crisis management team' to address sudden and unanticipated events.
viii. Maintaining effective liaison with media and issuing prompt clarifications or rebuttals to negative reports.

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 and reviewed by the Top Management.

7. 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, conflicts in West Asia have further demonstrated the importance of preparing proactively for catastrophes that seem implausible but are probable.

7.1. 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 (Eg. 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.

7.2 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.

7.3 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.

7.4 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. Inter dependencies 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 centre 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.

7.5 Existential risk governance

Existential risk management programme 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 co-ordinated 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.

Residual risks

While it is impossible to eliminate all of an organization's risk exposure, the risk framework help 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, Risk, Compliance and Audit team continually monitor adherence to various risk points affecting the company, the risk tolerance parameters need be modified subject to changes in the market and risks being faced by the organization. Senior Management reviews the risk tolerance parameters on an ongoing basis and suggest new parameters within which risk in the company to be managed.

8. Risk Governance in the Company

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

8.1. 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 (CCC)

Segregation of duties across the 'three lines of defence' 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.

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

8.2.1. 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 of

Three directors of the Board

The Chief Risk Officer will be a permanent invitee along with MD,CFO & CEO

Company Secretary shall be Secretary of the RMCB.

RMCB shall always be chaired by a 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

8.2.2. 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.

8.2.3. 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 organisational 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 stress 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.

9. 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

9.1. 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

9.1.1 Asset- Liability Management Committee (ALCO): The ALCO consisting of 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, decision 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 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 .

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

- Compliance to 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 scenario' and preparation of contingency plans.
- Adequacy of hedging forex exposures.
- Interest rate sensitivity

9.1.2Central Credit Committee (CCC)

CCC shall be responsible for ensuring credit quality of the portfolio, setting tolerance limits for various parameters in the portfolio and evaluating credit worthiness of high value credit proposals of Rs 20.00 lakhs and above.

Responsibilities of CCC

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

Quorum of CCC: CEO/CFO,CRO & the Head of Business unit concerned, will 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 .

9.1.3 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 Outsourcing Committee

i. Review of all outsourcing arrangements, as per the periodicity stipulated by the RBI
ii. To evaluate the risks involved in the outsourcing arrangements
iii. To review the audit reports of outsourcing arrangements
iv. To ensure that all the outsourcing arraignments 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 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.

9.2. 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.

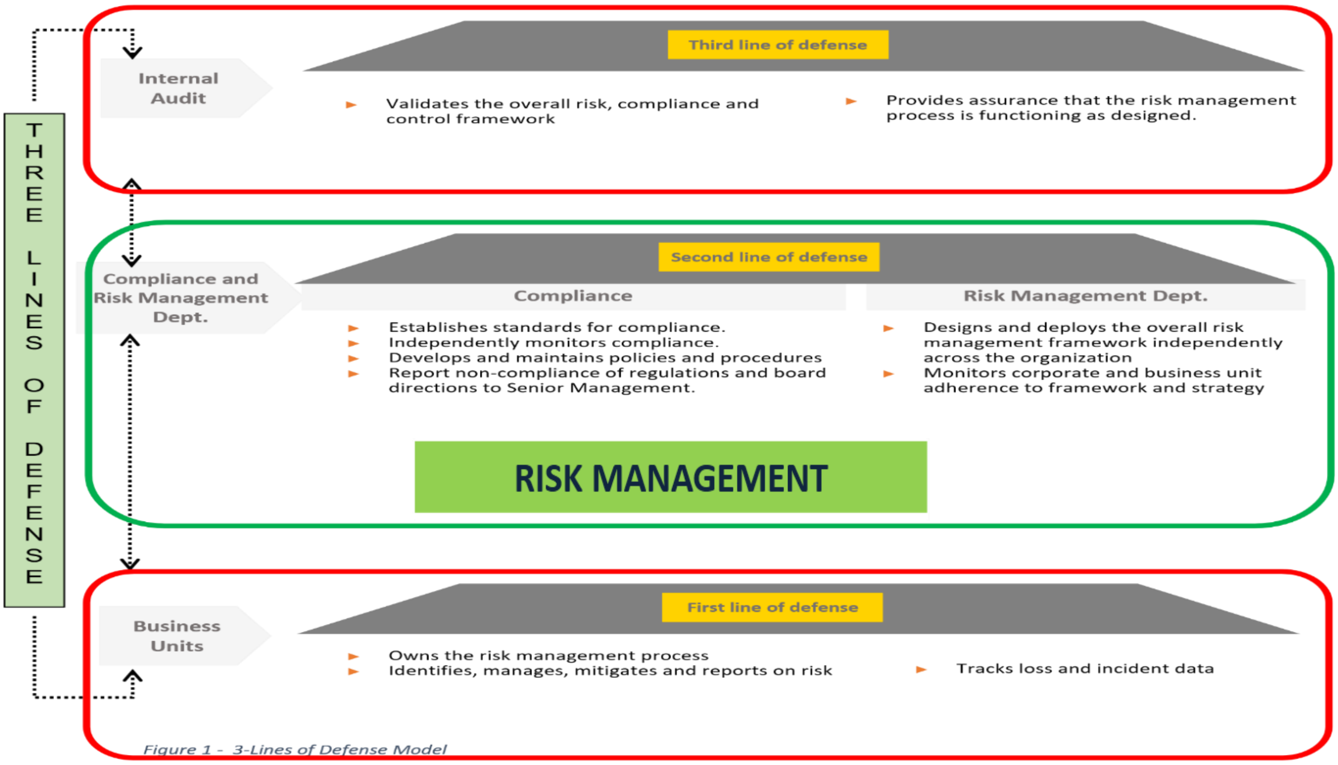


Figure 1 - 3-Lines of Defense Model

9.3. 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.

9.4. The Risk Management Department

The RMD of the company will be an advisory guide for all Risk related matters to all business and supports 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.

9.5. The Organization Chart of the Department

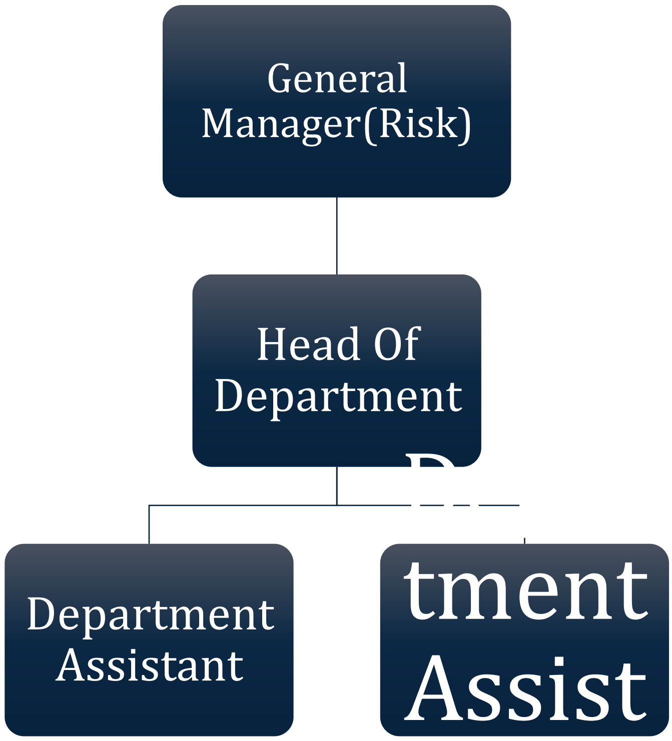


Figure 1 - Organization Chart of Risk Management Dept

9.6 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 risk angle.
- Vetting credit proposals from 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

10. 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.

10.1. 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.

10.2. 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. Reporting to the Managing Director & the Board of Directors on Risks

10.3 Risk Adjusted Return on Capital (RAROC)

Risk-adjusted return on capital (RAROC) is a risk-based profitability measurement framework for analysing 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.

10.4. 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.

11.Others

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

11.2. 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 harmonised 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.

Economic Risk

In simple terminology "Economic Risk (ER)" can be explained as the possibility that an economic downturn will negatively impact the ongoing business and or investments.

The risk that arises from the economic factors on the investments of the business. Factors which could restraints growth such as economic development (gross domestic product), exchange rate, fiscal deficit, monetary policy, consumer price index etc… influencing the amount of risk associated with the investment. Countries with stable economic growth have less risk as compared to those countries which have high volatility in growth rate.

Key Economic Risk indicators and its impacts

Economic indicators can be classified into two types Leading indicators and Lagging indicators:

Leading indicators often changes to large economic adjustments and, as such, can be used to predict future trends. For example: Stock Market performance, manufacturing production, Index of Industrial Production (IIP), etc…

The lead indicators help us to predict the future trend of the economy. Repo Rate is considering to be the good leading indicator of the liquidity in the economy and the bank lending rate to their borrowers. This will have a direct impact on the cost of borrowing of the borrowers.

Lagging indicators reflect the economy's historical performance and changes to these are only identifiable after an economic trend or pattern has already been established. For example: Gross Domestic Product (GDP), Consumer Price Index (CPI), Wholesale Price Index (WPI), Unemployment rate, Interest Rate etc…

A lagging indicators helps us understand how the parameters/ variables have behaved over the period of time under observation. The importance of a lagging indicator is its ability to confirm that a pattern is occurring.

Unemployment is one of the most popular lagging indicators. If the unemployment rate is rising, it indicates that the economy has not been doing well. Another example of a lagging indicator is the Consumer Price Index (CPI) which measures changes in the price level which impact the disposable income or the purchasing capability of an individual.

The economic indicators help the business prepare to take necessary strategic action by estimating the economic activities and position the business operations to protect or take advantage of the given economic scenario(s). Some of the key economic indicators and its impact on the business are explained below.

Key leading indicators and its impact Stock Market

The performance of stock market is the key leading indicator for the foreign investors investing in the country. The stock market help understands the direction at which the economic growth is expected to take place. Since stock prices reflects the performance of the companies and it's expected earn growth, the market can indicate the economic performance if earnings estimates are accurate.

For our verticals like loan against property for even commercial vehicle finance the performance of the stock market would provide key indicator how the sectors are performing and how it is expected to do. The performance of small business or medium size business can be measured by using the generalise Small cap index, Mid cap index as a proxy for sector growth. This will help up appraise the customer's operation with the overall sector growth.

Index of Industrial Production (IIP)

The Index of Industrial Production (IIP) gives details about the growth of various sectors in an economy such as mineral mining, electricity and manufacturing. The all India IIP is a composite indicator that measures the short-term changes in the volume of production of a basket of industrial products during a given period with respect to that in a chosen base period. It is compiled and published monthly by the central statistical organisation (CSO), Ministry of Statistics and Programme Implementation (MOSPI) six weeks after the reference month ends.

The index will help measure the performance of the sector and in all economic growth of the country. It is widely watched by various policy makers like the Finance Ministry and the Reserve Bank of India (RBI) and industry association like FICCI, CII etc. to estimate the business performance. Automobile Industry Performance

The Automobile industry has the cyclical business and reflects the economic performance of the country. Sales in the automotive sector are higher when economic activity is growing and there is strong customer sentiment about their future economic prospects. The automobile industry is also a proxy for the state of infrastructure where high-growth economies require better means of transportation and faster mobility.

The consumer business sentiment and also its disposable income can be measures through auto sales. The auto sells like two wheelers, tractors etc. is the proxy for the rural income and the demand estimate for observed period.

Bond Market

The bond market is a good predictor of future economic activity and future levels of inflation, both of which directly affect the price. The bond yield and bond price moves in opposite direction. The direction in bond market also helps the trend in which the government borrowing programme is expected to behave. Higher government borrowing programme will impact fiscal budget for the year which will impact the economic growth.

The bond market will impact the investment decision and the liquidity in the market which indirectly impact the cost of borrowing for the corporate sector.

Key lagging indicators and its impact Gross Domestic Product (GDP)

The gross domestic product is the comprehensive scorecard of the country's economic health. As an aggregate measure of total economic production for a country, GDP represents the market value of all goods and services produced by the economy during the period measured, including personal consumption, government purchases, private inventories, and the foreign trade balance (net of exports and imports).

Company's business plan is directly related to the economic growth of the country. The state of economy or its economic cycle will determine the industry business cycle. The factors affecting economic growth like government policies will have direct impact of corporate business plans.

Consumer Price Index (CPI)

The Consumer Price Index (CPI) measures changes in the price level of basket of consumer goods and services purchased by households. The annual percentage change in a CPI is used as a measure of inflation.

The CPI determines the disposable income of the individual household. The purchasing power of the individual increase with the fall in the CPI rate and vice versa.
This is one of the main ingredient for demand of a commodity or service.

Current Account Deficit (CAD)

The current account deficit is a measurement of a country's trade where the value of the goods and services it imports exceeds the value of the goods and services it exports. The CAD as a percent of GDP is one of the key component in determining the health of the economy. High CAD will result in loss of forex reserves and the values of the domestic currency depreciate.

The CAD plays import role in government and RBI policy making. Since high forex reserves are utilised to protect the depreciating currency due to increase CAD. Many policy measures are undertaken to prevent high deficit which impact company's business growth. Gold is the second largest imported item in the Balance of Payment (BoP). Import duty has been imposed to restrict high consumption of imported gold.
The stress on BoP is already visible with the INR depreciating more than 4% this year.

External Factors - Crude Oil Price

Higher international crude price directly impacts the inflation level in the country. India is the third largest consumer of the crude oil. Any increase in crude oil price will have direct impact of the economic health of the country.

High oil price increases input cost pressures stemming from firmer metal prices and a weaker rupee are forcing manufacturers to pass them on to consumers. Inflation in the transport and communication sub-group accelerated due to the firming up of crude prices, even though the domestic pass-through to petrol and diesel was incomplete. Recently RBI raise its key policy rate mainly due to high international oil price which impact inflation level. The Economic Survey, 2018-19 estimates that a $ 10 per barrel increase in the price of crude reduces growth by 0.2-0.3 percentage points.

Policy rate in Advance Economies.

The changes in the key policy rate (interest rate) impact the domestic economy indirectly through capital outflow. For e.g. US Federal Reserve increase the interest rate foreign investors would withdraw their investment form risky assets to more safe heaven investment like US bonds and stocks.

The risk of liquidity crunch in the economy through capital outflow impact domestic currency valuation. The cost of borrowing for the corporate increases and the investment in the business slows down.

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.

****