MANAPPURAM FINANCE LIMITED (MAFIL)

# ENTERPRISE RISK MANAGEMENT (ERM) POLICY & FRAMEWORK

| Version Control | | |
|---|---|---|
| **Version Number** | **Description** | **Date** |
| Version 1 | Risk Management Policy | 09-08-2013 |
| Version 1.1 | Risk Management Policy | 07-02-2014 |
| Version 2 | ERM Policy & Framework | 16-10-2018 |
| Version 2.1 | ERM Policy & Framework | 27-01-2020 |
| Version 2.2 | ERM Policy & Framework | 29-01-2021 |
| | Amendment | 26-05-2021 |
| Version 2.3 | ERM Policy & Framework | 04-08-2022 |
| Version 2.4 | ERM Policy & Framework | 10-08-2023 |
| Version 2.5 | ERM Policy & Framework | 04-11-2024 |
| Version 2.6 | Renewal | 03-11-2025 |

**Effective Date : 10-08-2013**

**Next Review Date : 03-11-2026**

**Policy Owner : Head - Risk Management Department**

**Prepared by : Risk Management Department**

**Reviewed by : Policy Review Committee**

**Approved by : The Board**

# Contents

# 1. Introduction

Manappuram Finance Ltd. (MAFIL- with effect from 22 June 2011), have been in the business of gold loans from the 1986. The Company had floated a public issue in the year 1995.

While the core business of the Company continues *to be* of Gold Loans, currently MAFIL offers a diversified product portfolio including gold loans, MSME / SME finance, vehicle and equipment finance, personal loans, home improvement loans, corporate loans and on-lending to smaller NBFCs / MFIs and HFCs. MAFIL also render fee based services like domestic and international Money Transfers, Prepaid Payment Instruments (**PPIs**) and sale and purchase of Foreign Exchange.

Board in its meeting dt. 16/10/2018 approved a comprehensive Enterprise Risk Management Policy and Framework, revising the earlier risk management policies. Subsequently, 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 policies, which inter alia includes the following:

A. ICAAP policy.
B. Credit Risk Management Policy.
C. Operation Risk Management Policy.
D. Liquidity Risk Management Policy.
E. Outsourcing (Financial Services) Policy.
F. Outsourcing (IT) Policy.
G. Reputation Risk Management Policy.
H. Foreign Exchange Management Policy
I. Market Risk Management Policy (viz. ALM Policy, Resources Management Policy)

## 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.”

MAFIL adopts this globally accepted definition and will be guided by the philosophy 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, enable the Company to make consistently profitable and prudent business decisions across all its offices and ensure an acceptable risk-adjusted return on capital (RAROC)[1], 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 to acquire and maintain a pre-eminent position amongst NBFCs.

## 3. Risk Management Approach

Pillars of ERM

As mentioned, Enterprise Risk Management, ERM, looks at risk management from the perspective of the entire organisation. It identifies and assesses potential losses, dangers, hazards and other potentially harmful factors that may prevent the organisation 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 organisational strategy.

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 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 that we operate.

Responding to Identified risks: once the universe of risk has been identified and assessed it is necessary to develop risk management plans for risk mitigation. The process of identification and assessment may indicate a need for tighter internal controls and possible opportunities which may be of benefit to the firm.

Control activities and monitoring: This pillar covers establishing and maintaining internal controls that manage and monitor risks.

[1] Please refer to details on RAROC under Risk Reporting Section of this framework document.

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 optimise 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 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** (See Annexure 002)
    a. Macro-Economic Indicators affecting our businesses
    b. Micro Economic Indicators influencing our businesses
2. **Strategic Analyses**
    a. Business Analyses – including Industry Analyses
    b. Forecasting & Modelling – including techniques and thresholds
    c. Statistical Analyses – 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, MAFIL will continue this approach to the 'conventional risk management' practice.

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

- Credit Risk
- Market Risk
- Operational Risk
- Liquidity Risk

MAFIL 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 MAFIL 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 Current Status and Vision for Way Forward:

#### 5.1.2.1 Current Status:

Credit risk – for MAFIL'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. 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.

MAFIL generally extends gold loans for a period of 12 months. 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 inter alia.

#### 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) that is envisaged it is imperative that the risks are managed by introducing stringent credit purveyance processes that encompass the entire gamut of the Credit Lifecycle as follows: –

- sourcing of the right clientele,
- structuring of products that would suit the selected markets / geographical- and demographical-profiles,
- credit assessment 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 honored, through the strengthening of the credit risk management team in MAFIL, as well as the other group companies.

### 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 process, creditworthiness of each customer, new or existing, assessment of the risks involved and ensuring a measured 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

MAFIL will at all times have a well-structured Credit Risk Management Policy and Procedure[2] that is duly supported by the Top Management and approved by the Board of Directors or by a committee appointed by them.

[2] See Credit Risk Management Policy document.

#### 5.1.4.1 Introduction & Scope of the Policy

The Credit Risk Management Policy should set out the guidelines, principles and approach to manage credit risks for MAFIL 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 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 MAFIL.
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 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.

#### 5.1.4.3 Policy Administration Process

The Credit 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 credit risk management policy is to be flexible and responsive to changing market and regulatory conditions, it will be reviewed by the Head-Credit Risk and the Chief Risk Officer, from time to time and any revisions will be updated at least annually or as necessary. If clarification on interpretation is required, consultation must first be sought from the Risk function.

The Policy shall be reviewed by the Risk Management Committee of the Board and put up for approval by the Board of Directors at least annually. Exigencies, if any, shall be reported and approved by the Board of Directors through the RMCB at the next possible meeting.

## 5.2 Market Risk

### 5.2.1 Definition

Market Risk is defined as the risks arising from movements in interest rates and exchange rates, on the overall businesses of the company.

Risk Identified

### 5.2.2 Foreign Exchange Risk

MAFIL does not run a trading book in currencies. The foreign exchange risk that MAFIL exposed to out its non-trading book are as under:

Exchange risk on account of FFMC activities: Under AD II license from RBI, MAFIL sells and buys foreign bank notes from Tourists and to residents travelling abroad. Depending on the size of the stock being held the Company will face risk of movement of exchange rates leading to financial loss.

Mitigating plans: MAFIL's size of such exposures are less given the size of the stock being small. MAFIL monitors the risk by setting appropriate risk limit based on the risk appetite. If such exposure increases, the situation will be monitored and will seek to hedge the risk by disposing of the stock to wholesalers in the market.

Responsibility

The Asset Liability Management Committee (ALCO)[3] of MAFIL – 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 action.

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.

### 5.2.3 Interest Rate risk (IRR)

Though MAFIL does not run a trading book, it is exposed to interest rate movements on its borrowing and loans on account of the interest norms and also due to tenor mismatch of borrowing and loans.

Mitigating IRR

MAFIL follows procedure for management of IRR as guided by the SBR Master Directions, as amended from time to time. The procedure involves compiling IRR gap statement measuring the likely impact on account of 200 bps movement of

[3] See Annexure 01 for the Terms of Reference for ALCO

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

### 5.2.4 Liquidity Risk

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[4]. MAFIL has adopted a detailed Liquidity Risk Management Policy that would address any adverse situation on Liquidity position of the company.

## 5.3 Operational Risk

While most organizations spend their resources in managing Credit Risk and Market Risk, often it is the Operational Risk which needs to be managed most carefully, dimensioned and reviewed diligently.
Very often Operational Risks are bigger than Credit Risks and can deplete Net Worth/Capital very quickly. The allocation of appropriate levels of Capital to cover such risks has a direct influence through a higher capital cost and potentially reduce the ROA of the entire business.

The activities which MAFIL shall undertake, exposes it to various types of Operational Risks and hence MAFIL 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

### 5.3.1 Operational Risk – Definition

"Operational Risk is the risk of losses arising from failed or inadequate processes, systems, people and due to external events. Operational risk is defined as the risk

[4] See Liquidity Risks Management Policy of MAFIL

of loss resulting from inadequate or failed internal processes, people and systems or from external events.

This definition includes legal risk[5], but excludes strategic[6] and reputational risk[7].

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 Downtime / Access Controls / Capacity failures.
- **Vendor Management**: Non-Performance / Un Trained Personnel / SLA shortfalls.
- **Compliance Risks**: Regulatory / Legal / Internal Guidelines.

[5] Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.
[6] See Other Risks (Other than OR/CR/MR)
[7] See Other Risks (Other than OR/CR/MR)

### 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 Operational Risk Management Department (ORMD) 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 ORMD will also be using various MIS reports for RCSA, KRI and Loss data for reporting to the Board 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

The Operational Risk Management Policy aims at the following:

- Meet or exceed Reserve Bank of India (RBI) and Basel Committee requirements on Operational Risk Management in MAFIL.
- Assign clear accountability and responsibility for management and mitigation of Operational Risk
- Develop a common understanding of Operational Risks across MAFIL, to assess exposure with respect to Operational Risks and take appropriate actions
- Strengthen the internal control environment throughout MAFIL 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 MAFIL.
- Compute capital charge for Operational Risk as per the Basel Committee 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

**ORM Governance**: Operational Risk Management (ORM) governance structure includes Board of Directors, and Operation Risk Management Committee (ORMC).

**ORM Policy and Procedures:** ORM Policy and related processes will be prepared by the Head – Operational Risk Management and the Chief Risk Officer and will cover Risk and Control Self-Assessment (RCSA), Key Risk Indicator (KRI), Loss Data Management (LDM) – and will be separately documented and approved by the RMCB and the Board.

**ORM Organization Structure:** MAFIL's Organizational structure for managing operation risks consists of the following three lines of defence.

- First line of Defense consists of functions that own and manage risk which in MAFIL 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 MAFIL 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, internal controls.

**ORM Assessment and Measurement Tools:** The primary tool for measuring operational risk across MAFIL shall include internal operational loss data. These loss data are used primarily for assessing and monitoring operational risk exposures across MAFIL. ORMC 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 ORMC 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, ORMC, 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 MAFIL for the required data to prepare the above report.

### 5.3.3 Operational Risk Appetite

MAFIL 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 ORMC.

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 – Operational Risk will draw up a detailed process document[8] 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.

### 5.3.4 Other Operational Risk Elements

#### 5.3.4.1 Outsourcing of Activities

Non-core functions[9] [10]may be outsourced to reputed and approved agencies which 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 security of offices, dispatch of bulk letters, premises cleaning, 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.

[8] Please refer to Risk Appetite and Tolerance Policy and Framework.
[9] Please refer Outsourcing Policy & Framework – for details on what can be and cannot be outsourced;
[10] Outsourcing of Activities will always be governed by the extant RBI Guidelines (currently No: RBI/2017-18/87 DNBR.PD.CC. No.090/03.10.001/2017-18 dated 09 November 2017).

#### 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 its 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.

MAFIL adopts the guidelines enshrined in the ISO Standard 22301 – the Global standard for Business Continuity Management Systems.

The BCMS Methodology should compulsorily include the Business Impact Analysis and the Risk Assessment. These processes should be detailed in the BCMS Policy and Procedures Framework of the Company.

The BCMS Policy and Procedures Framework shall be reviewed (and revised as may be appropriate and necessary) by the Chief Risk Officer / Head – Risk Management, from time to time – in line with both the ISO 22301 and the Good Practices Guidelines of The Business Continuity Institute, UK, and – in line with the extant RBI Guidelines[11]

[11] RBI's Circular RBI/2012-13/547 DIT.CO (Policy) No. 2636/09.63.025/2012-13 dated 26th June 2013

#### 5.3.4.4 Risk Based Internal Audit (RBIA)

MAFIL adopts the RBIA guidelines[12] of RBI as a part of its Operational Risk Management Framework.

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

RBIA allows 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 to help management achieve their 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 will 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 adoption of a fully computerized environment for conducting its business operations. Considering the emerging challenges and business requirements since April 2011, the responsibility for managing the IT platform was entrusted to a reputed multinational company – IBM upto February 2022. After termination of the contract with IBM, the platform is managed by MACOM supported by ORACLE and SIFY. The Company will adopt a Comprehensive IT Policy[13] 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 located in Mumbai and DR is located in Hyderabad. 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 effected 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 / broadbands 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. Uninterruptible power supply (UPS) will be ensured at all offices.

[12] RBIA circular DBS.CO.PP.BC.10/11.01.005/2002-03 dated December 27, 2002
[13] Please refer to the IT Policy

e) **Data storage and access:** Database server gets updated online. Only authorized personnel will have access to the data base. Scope to tamper or alter the database will be eliminated through controls. 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 in to 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 Policy shall lay down safeguards that MAFIL shall apply to its information resources and assets to mitigate various cyber security risks. MAFIL shall implement security controls at all levels to protect the confidentiality, integrity and availability of information during processing, handling, transmission and storage. MAFIL 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:***

MAFIL 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 arrangement with group entities).
- Engagement of Service Providers: MAFIL 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: MAFIL shall enter into legally binding agreements defining the rights and obligations of each of the service providers.
- Risk Management: MAFIL 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 MAFIL 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: MAFIL shall ensure that their service providers have a robust framework for maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan. It shall evaluate the possibly of bringing the outsourced activity back in-house in an emergency situation. In the event of an unexpected terminations 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.

### 5.3.4.8 Safeguards for borrower data security for digital lending.

**Collection, usage and sharing of data with third parties**

- MAFIL shall ensure that any collection of data by own Digital Lending Applications (DLAs) and DLAs of Lending Service Providers (LSP) is need-based and with prior and explicit

consent of the borrower having audit trail. In any case, MAFIL shall also ensure that DLAs desist from accessing mobile phone resources like file and media, contact list, call logs, telephony functions, *etc.* A one-time access can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/ KYC requirements only, with the explicit consent of the borrower.

- The borrower shall be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the app delete/ forget the data.
- The purpose of obtaining borrowers' consent needs to be disclosed at each stage of interface with the borrowers.
- Explicit consent of the borrower shall be taken before sharing personal information with any third party, except for cases where such sharing is required as per statutory or regulatory requirement.

**Storage of data**

With regard to storage of data, MAFIL shall ensure the following:

- MAFIL and LSPs/DLAs engaged by them do not store personal information of borrowers except some basic minimal data (*viz.,* name, address, contact details of the customer, *etc.*) that may be required to carry out their operations. Responsibility regarding data privacy and security of the customer's personal information will be that of MAFIL.
- MAFIL shall have clear policy guidelines regarding the storage of customer data including the type of data that can be stored, the length of time for which data can be stored, restrictions on the use of data, data destruction protocol, standards for handling security breach, *etc.*, and also disclosed by own DLAs and of the LSPs engaged prominently on their website and the apps at all times.
- No biometric data is stored/ collected in the systems associated with own DLAs / of LSPs, unless allowed under extant statutory guidelines.
- All data is stored only in servers located within India, while ensuring compliance with statutory obligations/ regulatory instructions.

**Comprehensive privacy policy**

- Besides having a comprehensive privacy policy, MAFIL shall ensure that their DLAs and LSPs engaged by them have a comprehensive privacy policy compliant with applicable laws, associated regulations and RBI guidelines. For access and collection of personal information of borrowers, DLAs of REs/LSPs should make the comprehensive privacy policy available publicly.

- Details of third parties (where applicable) allowed to collect personal information through the DLA shall also be disclosed in the privacy policy.

**Technology standards**

It shall be ensured that MAFIL and the LSPs engaged by them comply with various technology standards/ requirements on cybersecurity stipulated by RBI and other agencies, or as may be specified from time to time, for undertaking digital lending.

#### 5.3.4.9 Financial Crime Risk /Counter Terrorist Financing (FC/CTF) Risk

Counter Terrorist financing (CTF) are laws and regulations that aim to stop the illegal financing of terrorism and terrorist-related activities. It is closely tied to anti-money laundering (AML). MAFIL has been conducting transaction monitoring, filing of STR and CTR and KYC / AML risk assessment on a quarterly basis.

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

**Note:** To manage and mitigate operational risks that could result in financial loss or business disruption, MAFIL shall maintain appropriate insurance coverage and shall be reviewed periodically to ensure adequacy and alignment with the organizations risk profile and regulatory requirements.

## 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, SEBI, Stock Exchange and 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. Rising numbers and expectations of stakeholders, robust growth in the business of NBFCs, increasing dependency on non-equity sources of funding and some 'Corporate' frauds have increased the regulatory gaze, increased the complexity of the regulations and sometimes necessitate investments / costs.

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:

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. Institutionalising 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 / 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 (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.

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.
c. 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.
d. 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.<br>• Prepare the IT infrastructure facilitating to work from remote centers.<br>• 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.<br>• 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.<br>• MAFIL's data centre is located in Mumbai and Data Recovery Centre is located in Hyderabad. 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.<br>• All the physical assets are covered by insurance including, if available against tsunami kind of risks.<br>• The Company already have a warm site at Mumbai from where skeleton operations can be restored within limited time in the event of any disaster hitting to the HO.<br>• MAFIL already has a business continuity plan in which natural calamities also factored in. |

#### 5.4.3.4. 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 Senior Management. Accordingly, a committee for Existential risk management shall be in place comprising of MD&CEO, one or more members of the Board and two or three members from the KMP with appropriate standby in the event of the named persons are not available to contact. The committee 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 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.

### 5.4.4 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. MAFIL 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 MAFIL, 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 MAFIL to be managed.

# 6. Risk Governance in MAFIL

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

## 6.1. Key Principles of Risk Governance

MAFIL'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) and the Operation Risk Management Committee (ORMC).

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 MAFIL'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 MAFIL 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 MAFIL 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 Operation Risk Management Committee (ORMC), the Outsourcing Committee & the New Product Approval Committee, shall have presence of the Chief Risk Officer/Head – Risk Management 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 Organization 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

i) Three directors of the Board (of which at least two are independent directors)

ii) MD & CEO

The Chief Risk Officer / Head of Risk Management will be a permanent invitee along with CFO.

Company Secretary shall be 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 either two members or one third of the members of the committee, whichever is higher, including at least one member of the board of directors in attendance.

### 6.2.2. Frequency of Meeting

The RMCB shall meet at least 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 MAFIL, with or without power to delegate further.
4. Ensure appropriate risk organisation 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 MAFIL'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 MAFIL'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 extent internal policy guidelines and regulatory guidelines.
10. Review performance and set objectives for MAFIL's Chief Risk Officer / Head Risk Management and ensure he 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 listed entity, in particular including financial, operational, sectoral, sustainability (particularly, 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, at least once in two years, 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 Risk Management Committee.

The Risk Management Committee 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 Risk Management Committee 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)

MAFIL 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)
2. CREDIT Risks Committee : CCC (Central Credit Risk Committee)
3. OPERATIONAL Risks : ORMC (Operation Risk Management Committee)

The CRO/Head of Risk Management will prepare the Charter for each of these MRMCs and the MD & CEO 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 & CEO – Chairman<br>2. Executive Director<br>3. Chief Financial Officer<br>4. Head – Treasury / Funds Management (Secretary to ALCO)<br>5. Chief Technology Officer<br>6. Chief Risk Officer |
| 2. | CCC - Central Credit Risk Committee | 1. MD & CEO – Chairman<br>2. Executive Director<br>3. Chief Credit Officer<br>4. Chief Financial Officer<br>5. Chief Risk Officer<br>6. Head -Credit Risk Management (Secretary to CRMC) |
| 3. | Operation Risk Management Committee (ORMC) | 1. Chief Financial Officer<br>2. Chief Technology Officer/CISO<br>3. SVP – OGL & Technology Initiatives<br>4. SVP – Security & Administration/Premises<br>5. Chief Compliance Officer<br>6. GM – Human Resources<br>7. Head – Internal Audit<br>8. Chief Risk Officer / Dy. Chief Risk Officer<br>9. Chief Data Officer<br>10. Head - Legal<br>11. Heads of all business units<br>12. Head – Operational Risk Management (Secretary to the ORMC) |

**Note:**

MAFIL follows the practice of reviewing Operations Risks in Operation Risk Management Committee (ORMC) meetings as described in detail in the Operations Risk Management Policy.

### 6.3.2. Frequency of Meetings of ALCO:

ALCO will meet at least once in a quarter, and submit their reports including MOM to the RMCB, through the CRO, for review at its next quarterly meeting.

### 6.3.3. Terms of Reference of the MRMCs:

Please refer to Annexure 001 for the TOR for each of the MRMCs.

## 7. Management Structure of Risk Management in MAFIL

MAFIL adopts the "3 LINES OF DEFENSE MODEL" for the Management of its Risks. (See Figure 1)

- The 1st Line of Defense will always be the Business and Support Units that will own the risks and manage the same, as per laid down risk management guidelines.
- The 2nd Line of Defense will always be the Risk Management Department, the Compliance Department, and the Legal Department (sometimes collectively referred to as the Governance-Risk-Compliance Model or the GRC Model) that would support the 1st Line of Defense by the 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 the risk management principles/policies and processes are achieving the objective of managing the risks of the organization at all times.

Accordingly, the Company has set up a Risk Management Department (RMD) headed *a CRO /* Head – Risk Management for the purpose of managing risk related issues across the organization.

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

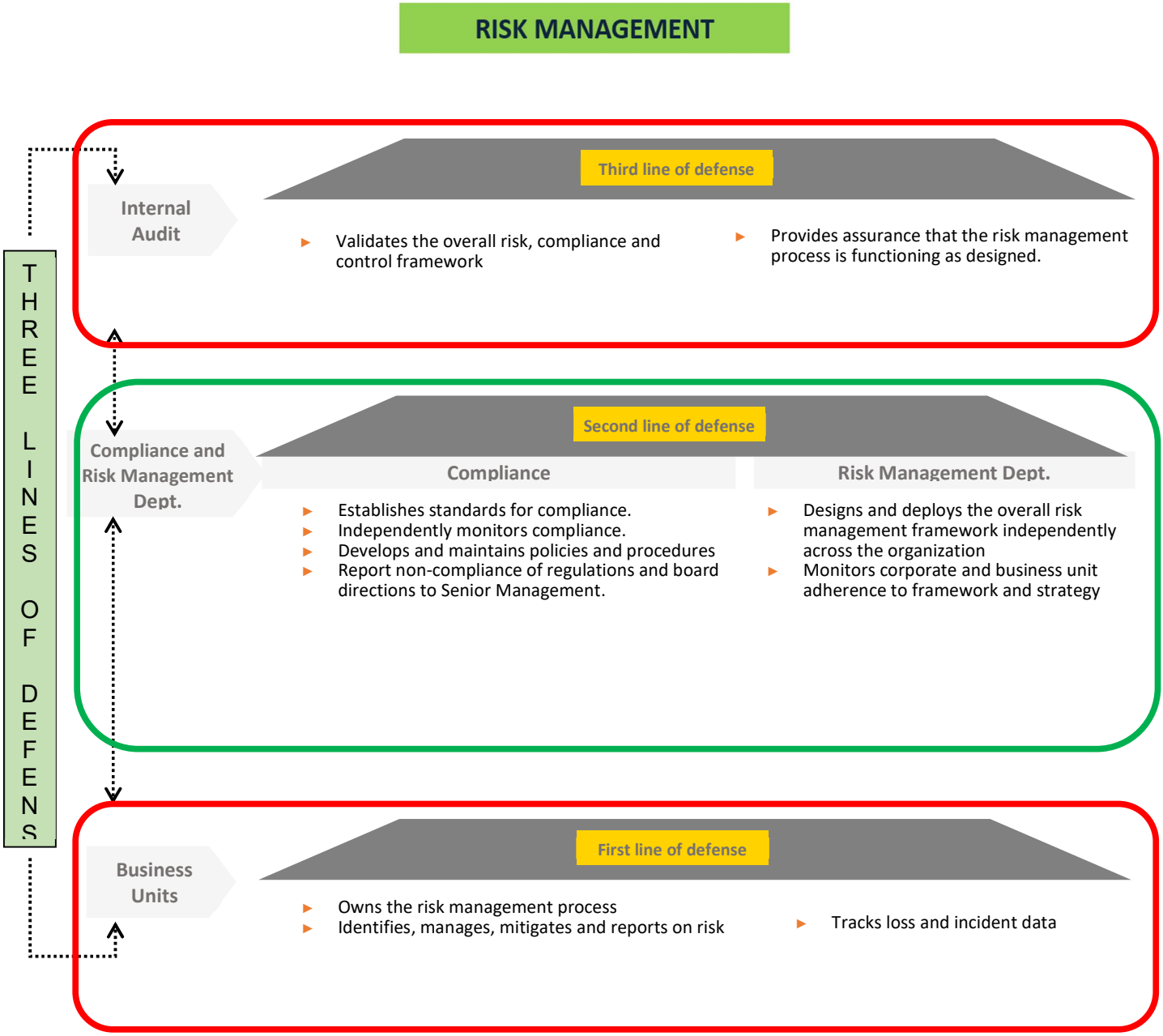



*Figure 1 - 3-Lines of Defense Model*

## 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.

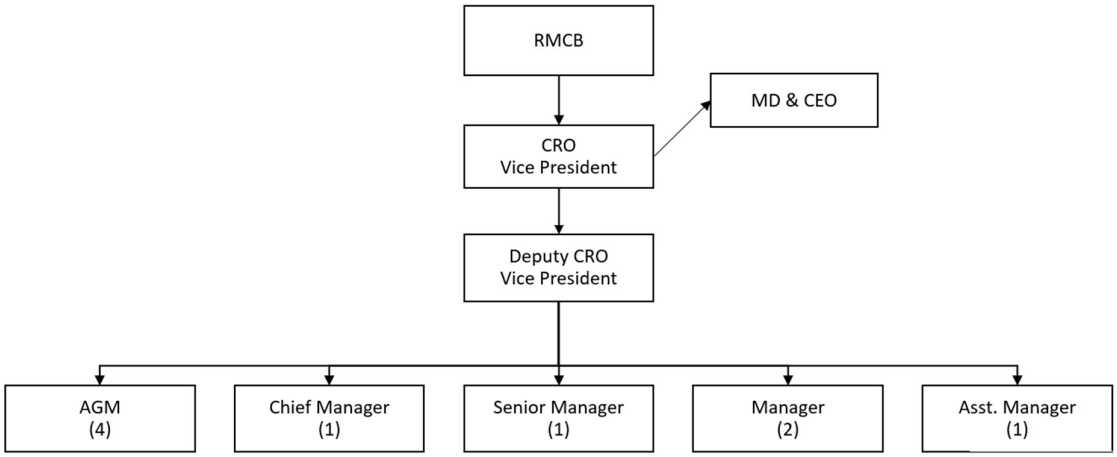
viii)Appraising uncovered / residual risks to the Management / Board.

## 7.2. The Risk Management Department Organization:

The RMD of MAFIL will be an advisory guide for all Risk related matters to all business and supports units in MAFIL and other group companies. 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 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 in risk angle.
- Vetting credit proposals in 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, Central Credit Risk Committee, outsourcing Committee and sanctioning committee of large credit proposals

# 8. ICAAP policy and document

Since introduction of Basel guidelines, Banks have been subjected to advanced level of capital assessment process based on their risk. G i ven the growing systemic importance of NBFCs, RBI through its Revised Regulatory Framework for NBFCs (Scale Based Regulations – SBR) has made applicable ICAAP requirements in the lines of banks for estimating their capital requirements. Brief details of the RBI stipulations as per circular number DOR.CRE.REC No. 60/03.10.0001/2021-22 dt October 22, 2021, are as below:

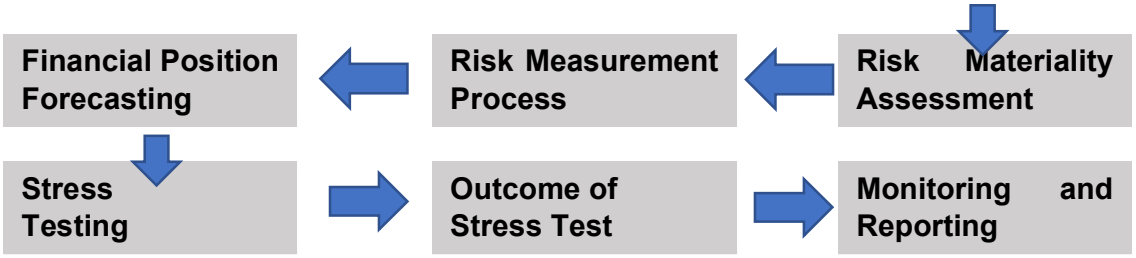
*Regulatory changes under SBR applicable to NBFC-ML and NBFC-UL: Internal Capital Adequacy Assessment Process (ICAAP) - NBFCs are required to make a thorough internal assessment of the need for capital, commensurate with the risks in their business. This internal assessment shall be on similar lines as ICAAP prescribed for commercial banks under Pillar 2 (Master Circular – Basel III Capital Regulations dated July 01, 2015).* ***While Pillar 2 capital will not be insisted upon****, NBFCs are required to make a realistic assessment of risks. Internal capital assessment shall factor in credit risk, market risk, operational risk and all other residual risks as per methodology to be determined internally. The methodology for internal assessment of capital shall be proportionate to the scale and complexity of operations as per their Board approved policy. The objective of ICAAP is to ensure availability of adequate capital to support all risks in business as also to encourage NBFCs to develop and use better internal risk management techniques for monitoring and managing their risks. This will facilitate an active dialogue between the supervisors and NBFCs on the assessment of risks and monitoring as well as mitigation of the same*.

RBI subsequent to its circular of 15 July 2015, issued a Master circular titled Basle III regulations ref No. RBI/2022-23/12 DOR.CAP.REC.3/21.06.201/2022-23 on 1 April 2022 combining various circulars published after 15th July 2015. (Subsequently, RBI on 12th May 2023 updated the Master Circular). RBI has indicated in the SBR that the process for NBFCs will be in line with its directive of July 2015 applicable to Banks. Accordingly, MAFIL has put in place the ICAAP policy in compliance with the RBI directions contained in the Circular dated 22 October 2021 and in alignment with the Basel III Master Circular dated 1 April 2022. (Approved by the Board of Directors in meeting dt 12th November 2022).

## 8.1 ICAAP structure

An illustrative depiction of the ICAAP structure is given in the following table.

| | | |
|---|---|---|
| **ICAAP Policy** | **Risk Identification** | **Risk Quantification** |




## 8.2 Material risks in MAFIL

Capital allocation for risks is considered based on the following methodology

| Sl no. | Risk | Description/methodology adopted |
|---|---|---|
| 1 | Credit Risk | Computed based on the regulatory approach. |
| 2 | Market Risk | Computed based on the regulatory approach. MAFIL does not have exposures in trading book currently and hence as of now capital assessment for Market risk is not applicable. |
| 3 | Operational Risk | Computed based on the regulatory approach.<br>For stress testing, operational risk capital is estimated using the Basic Indicator Approach (BIA), which is generally used by Banks for their Operational Risk Capital estimation. |
| 4 | Interest rate risk in the banking book (IRRBB) | For stress testing, MAFIL may adopt NII (Earnings at Risk) and EVE (Duration gap analysis) approach based on the Parallel shock scenario of the RBI IRRBB guidelines. |
| 5 | Credit concentration risk | For stress testing, MAFIL may adopt Herfindahl Hirschman Index (HHI) methodology based on industry practice and qualitative indicators in order to assess the level of concentration in its credit portfolio. |
| 6 | Liquidity risk | MAFIL may consider the following approaches to assess the liquidity risk within its portfolio:<br>1. Assessment of additional cost for liquidity gap<br>2. Liquidity Coverage Ratio<br>3. Assessment of funding concentration risk |
| 7 | Reputational risk | MAFIL has developed a Reputational Risk Assessment Scorecard in order to assess the level of reputational risk. |
| 8 | Strategic risk | MAFIL has developed a Strategic Risk Assessment Scorecard in order to assess the level of strategic risk. |
| 9 | Risk of under-estimation of credit risk under the Standardized approach | In order to assess risk of under-estimation of credit risk, MAFIL may adopt Internal Risk Based (IRB) Approach based on RBI guidelines. MAFIL has used PD, LGD and EAD values based on its ECL model. |

| | | |
|---|---|---|
| 10 | Cyber security/IT infrastructure risk | MAFIL has adopted a Comprehensive IT Policy encompassing acceptability of various usages, asset management, applications management, infrastructure management and IT security. The Cyber Security Policy lays down safeguards that MAFIL shall apply to its information resources and assets to mitigate various cyber security risks. MAFIL shall further implement security controls at all levels to protect the confidentiality, integrity and availability of information during processing, handling, transmission and storage. MAFIL 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. MAFIL may provide capital based on the losses, if any emanated from cyber-attacks and other security events. |
| 11 | Human capital risk | Human capital risk is covered under operational and reputation risk. |
| 12 | Group risk | Group risk is covered under reputation risk. |
| 13 | Outsourcing / vendor management risk | 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. The Third-Party Risk (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. A detailed Outsourcing Policy and Procedures is approved by the Board and adhered to by the Company. MAFIL may provide capital based on the losses, if any emanated from outsourcing risks. |
| 14 | Climate risk | The company has formulated an ESG policy which defines its commitments towards environmental laws and policies, minimizing environmental impact by reducing our greenhouse gas emissions, conserving natural resources, and preventing pollution, assessing environmental performance and set targets to improve environmental performance. |
| 15 | Settlement risk | Non-material risk for MAFIL |
| 16 | Legal Risk | Non-material risk for MAFIL |
| 17 | Risk of weakness in the credit-risk mitigants | Non-material risk for MAFIL |
| 18 | Model risk i.e., the risk of under-estimation of | Non-material risk for MAFIL |

| | | |
|---|---|---|
| | credit risk under the IRB approaches | |
| 19 | Collateral risk | Non-material risk for MAFIL |
| 20 | Fraud risk | Non-material risk for MAFIL |
| 21 | Political risk | Non-material risk for MAFIL |
| 22 | Residual risk | Non-material risk for MAFIL |

## *8.3* Stress testing

While a Financial Institution typically manages Capital and liquidity under "normal" circumstances, it should be prepared to manage Capital and Liquidity under stressed conditions. MAFIL shall perform stress tests in order to identify and quantify its exposures to possible future capital and liquidity stresses, analyzing possible impacts on the institution's cash flows, liquidity position, profitability and solvency.

The results of these stress tests shall be discussed thoroughly by management. The results of stress tests also play a key role in shaping MAFIL's contingency planning and in determining the strategy and tactics to deal with events of stress.

## 8.4 Reporting of outcome of ICAAP to the Board and RBI

The ICAAP is an ongoing process and will require a report on the outcome to be prepared and reported to the Board and if sought for to the RBI. Risk Management Department shall prepare the assessment report (ICAAP document) covering the risks identified, the manner in which those risks are monitored and managed, the impact of the changing risk profile on the capital position, details of stress tests/scenario analysis conducted and the resultant capital requirements. The reports shall be sufficiently detailed to allow the Board of Directors to evaluate the level and trend of material risk exposures, whether the Company maintains adequate capital against the risk exposures and in case of additional capital being needed, the plan for augmenting capital. The board of directors would be expected make timely adjustments to the strategic plan, as necessary.

## 8.5 Review of the ICAAP Outcomes

The board of directors shall, at least once a year, assess and Assessment document to know whether the processes relating to the ICAAP implemented by MAFIL covers all aspects envisaged is able achieve any specific objectives envisaged by the board. Risk Management and members of the senior management shall also and review the reports regularly to evaluate the sensitivity of the key assumptions and to assess the validity of the Company's estimated future capital requirements. In the light of such an assessment, appropriate changes in the ICAAP shall be instituted to ensure that the underlying objectives are met.

Also, an annual review of the ICAAP shall be conducted by Internal Audit to ensure continued alignment with regulatory expectations and internal risk management standards.

# 9. 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.

## 9.1. 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.

## 9.2. 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.

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

#### 9.2.1.1. 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.

Going forward, MAFIL shall adopt Transfer Pricing (FTP) framework to analyse financial performance of Businesses.

#### 9.2.1.2. Periodic Reporting to RMCB

The CRO/Head – Risk Management 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.

## 10. **Others**

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

**10.2 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.

A dedicated Control Functions Working Group, comprising representatives from the risk management, compliance, vigilance, and internal audit functions, shall be formed to strengthen collaboration and support integrated risk oversight across the organization.

## Annexure 001: **Terms of Reference – Management Risk Management Committees**

### 1. ORMC (Operation Risk Management Committee)

- Review and approve policies, products / processes / systems & procedures etc. involving Operational Risk elements introduced from time to time
- Review the risk profile, understand future changes and threats, and prioritize action steps
- Review and approve the development and implementation of risk methodologies and tools, including assessments, reporting, capital and loss event databases
- Review and manage potential risks which may arise from regulatory changes/ or changes in economic / political environment in order to keep pace with the required changes
- Review and approve suitable controls/ mitigant for managing Operational Risk, Fraud Risk and IT&IS Risk
- Promote a risk aware culture within MAFIL and communicate to business areas and staff, the importance of Operational Risk Management
- Ensure adequate resources are being assigned to mitigate and manage risks as needed

### 2. CCC (Central Credit Risk Committee):

- Establish a governance framework to ensure an effective oversight, segregation of duties, monitoring and management of credit risk in the MAFIL.
- Lay down guiding principles for setting up & monitoring of the credit risk appetite & limits.
- Establish standards for internal credit scoring framework
- Establish standards for effective measurement and monitoring of credit risk
- Achieve a well-diversified portfolio enabled by concentration risk management and maintaining credit risk exposures within established credit limits.
- Establish principles for credit risk stress testing.
- Enable monitoring of credit risk by way of Early Warning Signals (EWS).
- Adhere to the guidelines/policies related to credit risk management, as issued by the Reserve Bank of India (RBI) from time to time.

3. ALCO (Asset Liability Management Committee)

- The Committee shall define the ALM & MR governance within the MAFIL
- Lay down the framework for identification, measurement and management of market risk, interest rate risk and liquidity risk in MAFIL
- The Committee shall review the new directives and regulatory limits for market risk, interest rate risk and liquidity risk monitoring. It shall also recommend revision in tolerance limits to the Board, as and when such revisions are deemed necessary.
- The Committee shall review the investment and market risk profile, interest rate profile and liquidity profile of MAFIL and ensure compliance with established internal and regulatory / prudential limits.
- Define framework for funding strategy, contingency planning and stress testing.
- Ensuring compliance of regulatory requirements.

## Annexure 002: **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.