MANAPPURAM FINANCE LIMITED (MAFIL)

RISK APPETITE AND TOLERANCE POLICY AND FRAMEWORK

Version Control		
Version Number	**Description**	**Date**
Version 0.1	Risk Appetite And Tolerance Policy And Framework	October 2018
Version 0.2	Risk Appetite And Tolerance Policy And Framework	January 2020
Version 0.3	Risk Appetite And Tolerance Policy And Framework	January 2021
Version 0.4	Risk Appetite And Tolerance Policy And Framework	February 2022
Version 0.5	Risk Appetite And Tolerance Policy And Framework	September 2022
Version 0.6	Risk Appetite And Tolerance Policy And Framework	February 2023

Effective Date : **03.02.2023**

Next Review Date : **03.02.2024**

Policy Owner : **Head – Risk Management**

Prepared By : **Risk Management Department**

Reviewed by : **Policy Review Committee**

Approved By : **MD & CEO, MAFIL.**

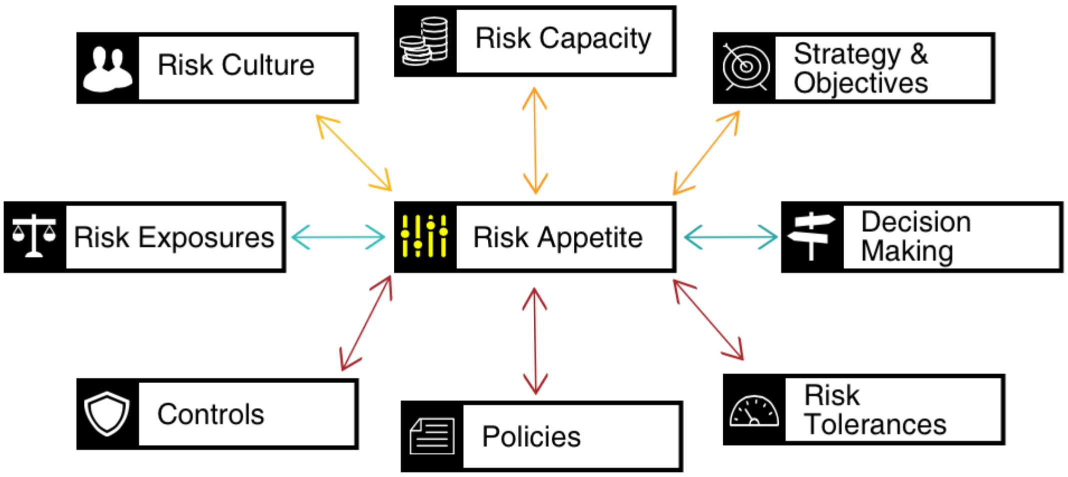
Contents

1. Introduction

The purpose of this document is to define and communicate key risk appetite related concepts and criteria, as covered within the risk appetite framework of MAFIL. It also aims to raise awareness of all the stake holders of MAFIL in taking and dealing with risks within the risk capacity.

The content of this document is to provide clear guidance to the reader on which risk exposures are acceptable and unacceptable to MAFIL. Such clarity can facilitate risk-informed decision making across MAFIL on risk related topics.

The diagram below highlights the various concepts that have been considered when defining the risk appetite of MAFIL



2. Objective

MAFIL has identified that the risk appetite statement should be a valuable reference in the following scenarios: -

- When an individual (being a staff member) or a business unit/vertical are making a significant business decision related to the business operations of MAFIL. Examples of such decisions may include, but not limited to, outsourcing significant processes or IT systems, acquiring new technology within products & expanding into new geographic locations, adding new product lines etc. In such scenarios, the concerned official/department/vertical should consider MAFIL's approach based on these guidelines whether the risks are acceptable or unacceptable.

- When an official/ department/ business unit/vertical carry out risk assessment of any proposal such assessment should inter alia identify whether the risk exposures are aligned and in conformity with MAFIL's approach towards acceptable and unacceptable operational risks.

- The rationale and approach behind the procedures followed in assessing the risk appetite shall be in alignment with the directions and guidance of the Risk Management Committee of the Board and to be explained in detail in case of a regulatory scrutiny.

3. Scope

The scope policy shall cover the following.

- New initiatives including introduction of new products, changing basic processes, initiatives for outsourcing, venturing into new geographies for expanding business new business tie ups.
- Existing activities will also come under the scope at the time of any review based on external events (any change in regulations and other external factors requiring a relook at the activities already pursued. etc).
- Initiatives to raise new debts should take cognizance of various covenants and other conditions fixed by the lenders and we are not likely to breach it. .
- Existing directions placed by Regulator in Inspections or other interventions and no tolerance on such matters shall be allowed.
- Adherence to conditions imposed by SEBI as part of Listing Obligations.

4. Risk Criteria

The guidance on acceptable and unacceptable risks is defined in the form of risk criteria, which are covered within this document. The risk criteria have been categorized into two levels, which are Level 1 & Level 2.

Level 1 provides guidance on risks that are unacceptable under any circumstances. Level 2 provides guidance on risk including operational risks that are avoidable prima facie but can be considered subject to overwhelming economic reasons as assessed by the Management. Such reasons broadly, but not limited to, as under: -

- The benefits both tangible and intangible derived by taking on the project/activity proposed is significantly high.
- Existing resources are not stretched.
- Adequacy of the existing risk management system to effectively manage the risks associated in case of takin up.

The following table covers the details of the various criteria that are applied to identify if exposure of a risk is in breach of MAFIL's risk appetite. Any risk that meets the criteria defined below should be covered within the "Risk Appetite Breach Report".

Level 1

- Features of unacceptable Risk in any circumstances

The Level 1 unacceptable risk criteria will have the following features

- Where the Activity / proposal if taken up/continued will lead to breaching one or more statutory or Regulatory prescriptions. Examples may include, but not limited to the following that may lead to: -
    - Mis-selling products/services to clients
    - Selling products/services to clients who are covered by national or international embargoes and sanctions
    - Misrepresenting or providing incorrect information to regulators or law enforcement agencies
    - Exposure that could breach regulatory limits.
    - Delinquency level of portfolios breaches corporate guidance.
    - Any breach in internal prudential limits prescribed in the loan policy.
    - Capital adequacy goes below the corporate aspirations.
    - Non compliance of any statutory guidelines in accounting, filing of returns etc.

- Where the Activity involves potential exposure to significant physical injury or loss of life for employees. Examples include: -
    - Harassment of employees by their managers or colleagues
    - Discrimination of employees by their managers or colleagues
    - Exposing employees to faulty machines or equipment leading to Health and safety related issues
    - Exposing employees to machines or equipment, where this may result in detrimental known impact on health of the employee

- Where the risk involves potential exposure to significant physical injury or loss of life for external stakeholders such as customers and suppliers. Only the risks owned by MAFIL should be considered. Examples include: -
    - Harassment of external stakeholders by staff or executives
    - Exposing external stakeholders to faulty machines or equipment
    - Exposing stakeholders to machines or equipment, where this may result in a known detrimental impact on health of the stakeholders

- Where the risk may breach MAFIL's s zero tolerance for the following types of fraud and corruption: -
    - Accepting or offering bribes by any employee
    - Embezzlement or misuse of assets for personal gains by employees and senior executives, including board members.
    - Financial statement fraud by employees and senior executives, including board members.

Level 2

Features of Level 2: -

- Risks which are avoidable under normal circumstances will be as under
  - The Overall risk assessed by Mail is "High" however;
  - MAFIL has resources to knowingly take the risk by effectively managing and;
  - the benefits associated vis a vis the risk carried with appropriate controls justifies the action
  - and that there are no Regulatory or statutory restrictions are in force

The following features shall be considered under this level: -

Customers

In respect of Customer impacting actions MAFIL shall have to take such calculated risk in the absence of which may result in the following;

- Customers being unable to access or operate their accounts held with MAFIL, due to system failure/downtime.
- MAFIL unintentionally providing incorrect information to customers regarding their accounts, funds or products.
- incorrect charges or transactions added to the customer accounts.
- unintentional damage (including theft) to customer funds and/or assets.
- increase in the level of yearly customer churn beyond the prescribed limits
- decrease in the level of new customer acquisition below the prescribed limits
- undervaluation of the asset of the customer.

Information & IT Systems

In respect of Information & IT systems impacting actions MAFIL shall have to take such calculated risk in the absence of which may result in the following

- unintended sharing information (e.g. about customers, employees, suppliers) with inappropriate individuals, business units or external organizations.
- disruption to key non-customer related IT Systems (e.g., Payroll Processing)

Statutory, Regulations & Obligations related

In respect of **Statutory, Regulations & Obligations related** impacting actions MAFIL shall have to take such calculated risk in the absence of which may result in the following

- MAFIL, unintentionally breaching one or more laws or regulations.
- MAFIL unintentionally breaching its contractual obligations to third parties.

Theft & Fraud

In respect of Theft & Fraud related impacting actions MAFIL shall have to take such calculated risk in the absence of which may result in the following

- theft or fraud committed by employees directly
- theft or fraud committed by external parties including customers

Employee

In respect of Employees related impacting actions MAFIL shall have to take such calculated risk in the absence of which may result in the following

- An increase in the level of staff turnover more than the prescribed levels

Financial
In respect of Financial impacting actions MAFIL shall have to take such calculated risk in the absence of which may result in the following

- total potential negative financial consequences of a risk are more than the prescribed levels the total budget of the business unit where the risk is owned.
- overvaluation of the asset of the customer

5. Responsibilities

5.1 Responsibility – Senior Management & Board

The Senior Management & The Risk Management Committee of Board of MAFIL shall have the responsibility for oversight of this policy and related activities to be undertaken under the policy. Senior management / RMCB shall review the risk tolerance parameters periodically and shall suggest variables in tune with dynamics of risks.

5.2 Responsibilities of Policy Owner

As delegated by the Board from time to time, the Policy Owner as constituted by the Board, the Chief Risk officer/Head-Risk Management shall have the overall responsibility to oversee and implement the policy as follows:

5.2.1 Ensuring the implementation of the Board's/Senior Management's decisions on this policy as applicable
5.2.2 Developing, implementing and periodically reviewing this policy and related procedures to ensure that it conforms to the scope of this policy.
5.2.3 Informing the Senior Management & Board on the all risks and provide periodical reports through "Risk Appetite Breach Report" (See Reporting Section of the ERM Framework)

5.3 Responsibilities of Units covered under the policy

The first line of defense provides that the business and operation units have in place effective processes to identify, assess, measure, monitor, mitigate, and report on their risks. Each unit operates in accordance with the risk policies and delegated mandates. The units are responsible for having skills, operating procedures, systems, and controls in place to ensure their compliance with risk policies and mandates.
It is the responsibility of All the HODs to ensure that the guidelines are followed as laid down in the policy in relation to the Risk Appetite & Tolerance levels to their respective unit, on key performance indicators. Any deviation required to in adhering to the guidelines of this policy should be approved by Owner of the Policy and Approver of the Policy.

6. Risk Appetite Breach Report

The Risk Appetite Breach Report is the main channel used for escalating risks to the board, risk committee, audit committee and senior executives. The report is created quarterly by the Risk Reporting team and made available via the Risk Dashboard

This report contains risks covered under the following levels defined earlier in this document: -

- Level 1
- Level 2

This report is presented to the following stakeholders: -

- Risk Committee/RMCB
- Audit Committee
- Heads of Departments, CEO, CRO, CFO etc.

Business Unit Level: The business units may maintain a KRI (Key Risk Indicator) & highlighting their risks & thresholds for their monitoring at unit level,

The format in which the KRI for the units to be prepared is as under:

<table>
<tr><th colspan="8">MANAPPURAM FINANCE LIMITED (MAFIL)</th></tr>
<tr><td rowspan="2">#</td><td>(NAME OF DEPT) XXXXX</td><td rowspan="2">Threshold</td><td colspan="4">FROM 1ST APRIL ……TO 31ST MAR ……</td><td rowspan="2">Brief Explanation & actionable if recommended threshold is breached</td></tr>
<tr><td>Key Risk Indicator</td><td>APR - JUN
QUARTER 1</td><td>JUL - SEP
QUARTER 2</td><td>OCT – DEC
QUARTER 3</td><td>JAN - MAR
QUARTER - 4</td></tr>
</table>

(The numbers/figures updated in the monthly columns need to be in **red** in case of breach of threshold)

7. Evaluating Threats & Opportunities

The current level of threat related measures is mainly used to include a risk within the Risk Appetite Breach Report. However, in certain cases the decision makers would also need to consider any opportunities corresponding to the threat related measures included in the report. Any decision related to implementation of further risk treatment for risks included in the report should be based on a balanced view of the level of threat and any corresponding opportunities. This will enable the decision makers to take a holistic view and balance the various strategic and operational objectives that may be influenced by the risk.

8. Implementing Risk Appetite through Risk Tolerances

Any business decision taken within MAFIL that may impact a given business objective should consider the defined thresholds. All business decisions should aim to maintain the performance within the defined thresholds. If a business decision needs to be taken which may breach the defined threshold, then the BU/SU level head is responsible for the business unit (where the decision needs to be taken) should justify & recommend such business decisions, with an approval from MD & CEO of MAFIL.

9. Implementing Risk Appetite through policies

The risk appetite levels and their associated criteria should also be implemented through new policies or clauses within existing policies, where appropriate.

Example: -

- The criteria defined in Level 1 around safety of employees and external stakeholders should be implemented through clauses within the Health & Safety Policy
- The criteria defined in Level 1 around zero tolerance for bribery should be implemented through clauses within the Anti-Bribery Policy.
- The criteria defined in Level 2 around unintentionally sharing customer information should be implemented through clauses within the Information Security Policy.

10. Implementing Risk Appetite through controls

The risk appetite levels and their associated criteria should also be implemented through implementation of controls, where appropriate.

Example: -

- The criteria defined in Level 1 around safety of employees and external stakeholders should be implemented through controls such as Fire Safety training, performing health and safety due diligence when buying new equipment etc.
- The criteria defined in Level 1 around zero tolerance for bribery should be implemented through controls such as yearly anti-bribery training, performing corruption related due diligence before starting conducting business with any external organization etc.
- The criteria defined in Level 2 around unintentionally sharing customer information should be implemented through controls such as classification of information based on level of confidentiality, approval process before authorizing an individual access to IT systems with sensitive information etc.

11. Aligning Risk Appetite with Risk Bearing Capacity

MAFIL has a finite amount of risk bearing capacity, which is defined as "The maximum level of resources MAFIL can outlay or expose in managing its risks without requiring a significant change to its business objectives and strategy".

As of now there is no Regulatory directives or any internal guidance for allocating capital specifically for the operational risks that MAFIL carries at any point in tie. However, with the introduction of Scale based Regulation it may become necessary to provide capital for all risks viz credit, Market, operational risks etc in line with ICAAP norms. As a gold lender MAFIL is likely to have savings in capital, (gold is a financial collateral which can be netted to exposures, with a haircut of 15%) once capital charge as per Basel III is introduced in NBFCs.

Accordingly, the risk bearing capacity of MAFIL vis a vis capital will be in place once the ICAAP driven model is evolved going forward. Given that MAFIL has high Capital Adequacy compared to its credit risks, the current capital is adequately cover all MAFIL's risks. Incremental load on the capital emanating from market and operational risks are to be tightly controlled with appropriate under overall control of the Board and Risk Management Committee.

12. Customise Risk Appetite Statement for Business Units

This risk appetite statement has been defined to be applicable for the company level and hence any context specific to business units has not been included. It is expected that individual business units will utilize this document as a basis for creating a risk appetite statement document for risk owners and other stakeholders within their business unit – if necessary, in consultation with the Chief Risk Officer/Head Risk Management. Such customized statements should include context information specific for the business unit, so its content can be relevant for the consumers of the statement within the business unit.

Such customization should retain the criteria defined within Level 1 of this document. New criteria can be added but existing criteria cannot be modified or removed. Business units can make any changes to criteria defined in all other levels.

If a business unit does not define a customized version of the risk appetite statement, then this document will be applicable for all risk appetite related activities (e.g. reporting) of such business units.

The format to be used by units & at entity level to identify performance indicators with acceptable risk Appetite/Tolerances – Annexure 1.

13. Monitoring Risk Appetite through Key Risk Indicator

Risk appetite breach Report including any breaches in the loan covenants thresholds shall be submitted to the Senior Management at periodical intervals. In addition, risk owners should also define one or more indicators for their risks to monitor potential or actual breach of any criteria defined earlier in this document. Continuous monitoring risks using such indicators aka known as Key Risk Indicator can provide risk owners with information on a timely basis. Without such information, risk owners may only find out about potential breaches during the quarterly assessments and this may sometimes restrict the amount of time available to risk owners for making decisions related to potential breach of risk appetite.

Examples of such Key Risk Indicator monitoring may include: -

- Number of whistle blowing issues reported.
- Number of new loss events reported.
- Number of exceptions raised for specific policies such as Gift Policy, Information Security Policy etc.
- Number of audit findings raised.
- Increase in delinquency in the portfolios.
- Deterioration in liquidity.
- Instances of breaches in individual/group exposure limits.
- Instances of breaching prudential ceilings for individual/ group exposure prescribed by regulators.
- Instances of breaches in mix of funding. (Liquidity risk)
- Instances of delay/default in repayment of debt by MAFIL.
- Instances of fines/adverse comments from regulators. viz; RBI, SEBI etc.
- Instances of breaches in any covenant thresholds set by Risk Management committee or any lenders to MAFIL.

14. Risk Appetite & Risk Culture

MAFIL defines risk culture as “Set of shared beliefs and values regarding management of risks”. MAFIL recognizes that risk culture is a very important factor driving the risk appetite. However, MAFIL also pro-actively intends to use the risk appetite to influence the risk culture, so the risk culture can facilitate MAFIL to achieve its business objectives.

15. Review of Risk Appetite Statements

The entity level and Unit Level Risk Appetite Statements may be reviewed when required as part of the overall Risk Framework.

16. Review of the policy

The Policy will be reviewed annually to ensure that the Policy remains current and relevant and with changes/amendments, as required & will follow the review / approval / ratification process.

This policy will be owned by the CRO/Head Risk Management who will be responsible for the maintenance of this policy.

Annexure-1: Risk Tolerance - List attached separately

Sl No	Key Risk Indicators	Impact	Metric Used	Tolerance Limit / Threshold	Actual Figures	Data Source / Department	Remarks

DISCUSSED & ACCEPTED BY

APPROVED BY