MUTHOOT CAPITAL SERVICES LIMITED

CIN: L67120KL1994PLC007726

ENTERPRISE RISK MANAGEMENT FRAMEWORK

Private and Confidential

This Policy was approved by the Board of Directors at the meeting held on 23rd January 2024 and reviewed on 23.05.2024

Version control:

Sl no	Name of the policy	Version	Board approval date	Remarks
1.	Enterprise Risk Management Framework	V1	23.01.2024	Policy document adopted
2.	Enterprise Risk Management Framework	V2	23.05.2024	Incorporated Points related to IT risk as per the latest IT governance policy.

TABLE OF CONTENTS

1. Introduction

Muthoot Capital Services Limited ("MCSL" or the "Company") promoted by the Muthoot Pappachan Group (MPG) is a Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India and listed on the BSE Limited and National Stock Exchange of India Limited.

Muthoot Capital Services Limited (MCSL) is primarily into the business of providing loans to individuals against the security of vehicles financed. In addition, company also lend unsecured loans and secured loans to corporate entities.

It is a well-known fact that an organization roots out the same pattern from the structure of a tree. As the organization grows, the risk associated with it begins to multiply. This necessitates a Risk Management Department in the organization.

The Risk department is required to ensure the safety of the organization from any and every threat against any uncertain events, Risk department educates the organization's stakeholders about the company's risk appetite.

There are two types of risk management techniques - Traditional Risk Management and Enterprise Risk Management

Muthoot Capital Services Limited (MCSL) made the decision to put Enterprise Risk Management (ERM) into place in order to examine the risks related to it. An ERM team collaborates with the business unit executives and personnel to debrief them, assist them in using the proper resources to consider the risks, compile their findings, and present them to the organization's executive leadership and board:

2. Enterprise Risk Management

Enterprise risk management (ERM) is the process of identifying and addressing methodically the potential events that represent risks to the achievement of strategic objectives, or to the opportunities for gaining competitive advantage, ERM draws a comprehensive approach and calls for management-level decision making that may be enigmatic for an individual business unit or segment. Thus, instead of each business unit being responsible for its own risk management, firm wide surveillance is kept on priority. For instance, if risk manager in a financial institution notice that two business units positioned in different areas of the company have similar exposures to the same risk, they may push the lesser important of the two to eradicate that position of risk.

A Chief Risk Officer (CRO), for instance, is a corporate executive position that is the foremost figure in the Risk department. The CRO is responsible for identifying, analyzing, and mitigating Internal and external risks. that impact the entire corporation. He/she also works to ensure that the company complies with government regulations and CRO's mandate will be specified in conjunction with other top management along with the Board of directors and other stakeholders.

3. Risk Management Philosophy

Muthoot Capital Services Limited (MCSL) revolves around the following Risk philosophy based on the 4 C's

1. Creating Risk Culture

2. Corporate Governance

3. Comprehensive and Pro-active Risk Management Process

4. Continuous monitoring

1) Creating Risk Culture

Risk culture is "the values, beliefs, knowledge and understanding about risk, shared by a group of people with a common purpose Risk culture is reflected in how the employees of the organization conduct themselves and their attitudes and approach towards Risk Management. A desired risk culture can be achieved by defining the desired risk culture, measuring the current state upon which gap analysis shall be done to achieve the targeted risk culture.

2) Corporate Governance

Corporate Governance is the overall system of rules, practices, and standards that guide a business. Enterprise risk management is the process of identifying threats or hazards to the business and acting to reduce or eliminate financial impact in the business.

3) Comprehensive and Proactive Risk Management Process

Risk management process, it identifies all potential threats within the business, whether they already exist or before and whether they generate a negative impact; analyses each threat, and determines its scope, potential and maximum disruption; evaluates, ranks and prioritizes each risk depending on its severity: formulates a plan to eliminate Or contain risk as much as possible by prioritizing risks to Highest to Lower level, and Risk mitigation strategy includes, avoiding the risk, reduce the likelihood of risk, mitigate, or cover the impact of risk and accept the risk

4) Continuous monitoring

Regularly monitor, track, and review risk mitigation results whether initiatives are adequate or further changes are supposed to be implemented.

4. Risk Management Principles

The Risk Management framework in **Muthoot Capital Services Limited (MCSL**) revolves around the following principles:

(i) identify and manage risks in line to the risk appetite and defined threshold limits to condense the uncertainty associated with the execution of the Company's vision, mission, and strategic objectives.

(ii) enhance MCSL's ability to create, preserve and realize value for its promoters and stakeholders.

(iii) ensure the risks are appropriate in relation to the scale and benefit of the business or practice or processes,

(iv) no individual risk or combination of risks result will end up with material impact to the financial performance, brand or reputation of the Company or Group

5. Risk Management Approach

Muthoot Capital Services Limited (MCSL) has defined below mentioned principles for adopting the approach for Enterprise Risk Framework:

1. Governance and Culture: Governance narrates the Company's approach, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity. It helps in exercising Board Risk Oversight, establishing operating structures, defines desired cultures, demonstrates commitment to Core Values and attracts, develops and retains capable individuals.

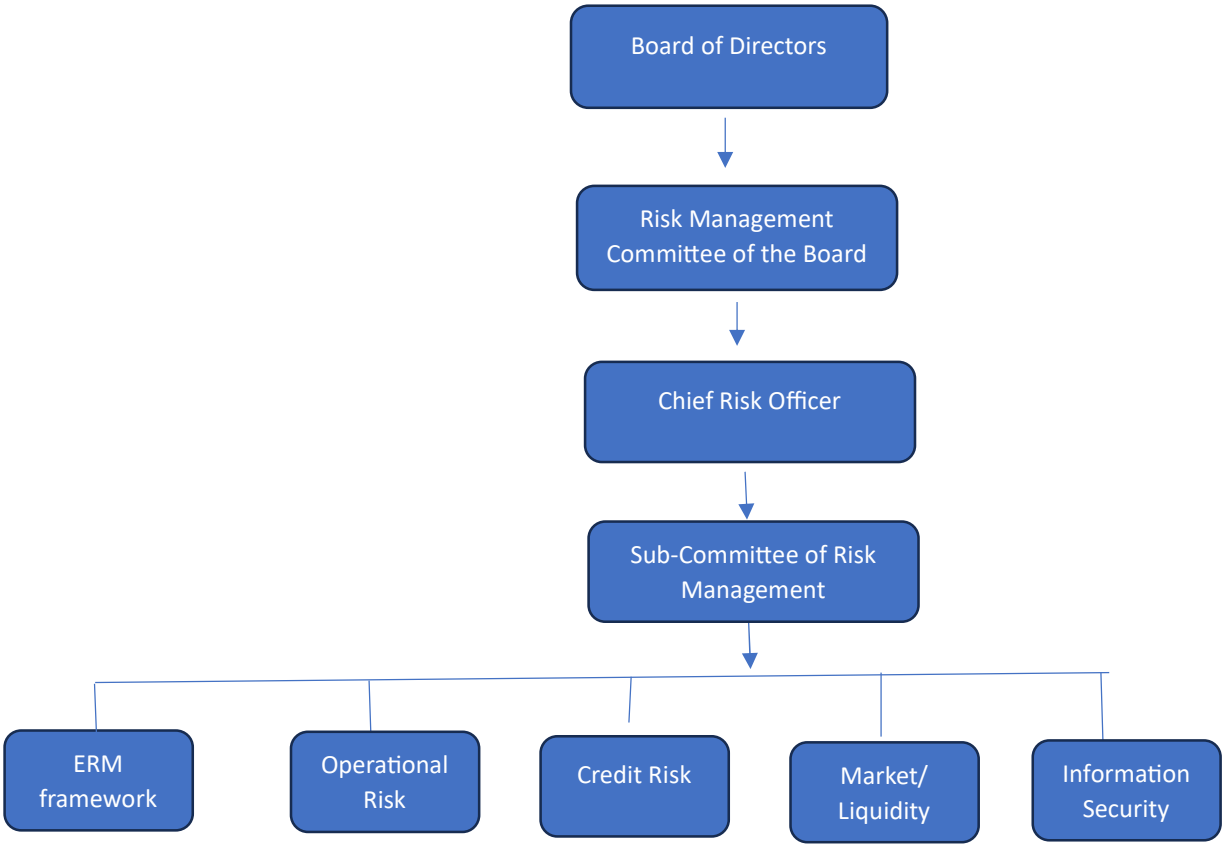
2. Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk. Analyzing business context, defining a risk appetite, evaluating alternative strategies and formulating business objectives are the main areas covered under the segment.

3. Performance: Risks that may impact on the achievement of Company's vision, mission, and strategic and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then evaluates risk responses and takes a portfolio view of the amount of risk and its severity. The results of this process are reported to key risk stakeholders. Identifying and assessing the severity of risk, prioritizing risks and implementing risk responses and developing a portfolio view are things that are viewed under performance.

4. Review and Revision: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed. Assessing substantial changes, reviews risk performance for pursuing Improvement in Enterprise Risk Management takes place in reviewing and revision sessions.

5. Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing adequate information, from both internal and external sources, which flows up, down, and across the organization. Leveraging information and Technology, communicating Risk Information and reports on risk, culture and performance are monitored under this segment.

6. Risk Management Structure



6.1 Role of the Board:

The Board plays a pivotal role in the effective management of the risk management process within the Company. The Board shall:

a) Be responsible for framing, implementing, and monitoring the risk management plan having in place, systems for risk management as part of internal controls with duty being cast upon Independent Directors to bring unbiased approach during the Board's deliberations on making risk management systems very strong and effective.

b) Define the roles and responsibilities of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the Committee and such other functions as it may deem fit;

c) Ensure that the appropriate systems for risk management are in place;

d) Ensure risk management is integrated into board reporting and annual reporting mechanisms;

e) Convene any board-committees that are deemed necessary to ensure risk is adequately managed and resolved where possible.

6.2 ROLES OF RISK MANAGEMENT COMMITTEE:

The terms of reference of the Risk Management Committee to be fixed by the Board shall include:

a) Oversee the development, implementation and maintenance of the Company's overall risk management framework and its appetite, strategy, principles and policies, to ensure they are in line with emerging regulatory, corporate governance and industry best practice;

b) Oversee the Company's risk exposures, risk/return and proposed improvements to the Group`s risk management framework and its risk appetite, strategy, principles, policies and standards;

c) Provide formal sign-off for the Board Risk Report and other risk related sections within the Annual Reports & Accounts.

d) Facilitate effective contribution and involvement of non-executives and aid their understanding of risk issues and the Company's risk management framework.

e) Provide input to the Remuneration Committee on the alignment of remuneration to risk performance.

f) review new risk principles and policy and material amendments to risk principles and policy recommended by the Chief Risk Officer ('CRO'), for approval by the Board;

g) oversee adherence to Company's risk principles, policies and standards and any action taken resulting from material policy breaches, based upon reports from the CRO;

h) i) Review the appointment, resignation or dismissal of the CRO and make appropriate recommendation to the Board;

ii) Review and discuss with the CRO the scope of work of the Company's Risk Division, its plans, the issues identified as a result of its work, how management is addressing these issues and the effectiveness of systems of risk management;

iii) Review the adequacy of the Company's Risk Division's resources, and its authority and standing within the company; and

iv) Review co-ordination between the Company's Risk Division and the external auditors; and

i) Periodically review and update its own terms of reference to reflect best practice, requesting Board approval for all proposed changes and, at appropriate intervals, evaluate its own performance against the terms of reference.

j) Review periodically the report of CRMC/ORMC/ Asset Liability Management Committee and to suggest on improvements, actions to be taken.

The Roles and responsibilities of Risk Management Committee in relation to ICAAP are listed below:

- Approving the ICAAP Procedures is in accordance with the framework laid down in the Board approved ICAAP Policy.
- Oversight of the ICAAP process including challenging the ICAAP and its underlying assumptions.
- Review and recommend for the approval of the Board, the proposed changes to the ICAAP Policy, methodologies developed by Risk and Finance functions.
- Review of identified material risk.
- Evaluating the level and trend of material risk and their effects on capital levels
- Reviewing the scope of coverage of the stress testing framework, risk factors, stress scenarios and the levels of stress applied.
- Integrating ICAAP with the capital planning and management procedures of MCSL
- Determining if MCSL holds adequate capital against the risks faced.
- Project the CRAR position based on the estimated business for the next three years detailing the proposed method for capital augmentation.
- Assessing future capital needs based on the risk profile of MCSL and proposing necessary adjustments to its strategic plan.

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 and employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise. if it considers necessary.

6.3 Responsibilities of the Risk Management Department (RMD)

Roles and responsibilities of the Risk Management Department are:

- Designing and putting into action an efficient risk management process for the organization, which includes an analysis of the financial impact on the company when risks occur.
- Performing a risk assessment: Analyzing current risks and identifying potential risks that are affecting the company.
- Performing a risk evaluation: Evaluating the company's previous handling of risks and comparing potential risks with criteria set out by the company such as costs and legal requirements.
- Establishing the level of risk, the company is willing to take.
- Risk reporting tailored to the relevant audience. (Educating the board of directors about the most significant risks to the business; ensuring business heads understand the risks that might affect their departments; ensuring individuals understand their own accountability for individual risks).
- Explaining the external risk posed by corporate governance to stakeholders.
- Conducting policy and compliance audits, which will include liaising with internal and external auditors.
- Reviewing any new major contracts or internal business proposals.
- Building risk awareness amongst staff by providing support and training within the company.

The Roles and responsibilities of Risk Management Department in relation to ICAAP are listed below:

- To be the focal point for RBI for the supervisory review process.
- To develop an ICAAP framework (policies, ICAAP document) in line with RBI guidelines.
- To present the board approved ICAAP to RBI along with the necessary supporting documents.
- To maintain all documentation supporting the ICAAP.
- Identification and assessment of all inherent and material risks.
- Devising appropriate methodologies for measurement of risks considering the nature, size, and complexity of Muthoot's operations, to measure the risk capital.
- Responsible for developing the methodology for the assessment of Pillar II risks.
- To define the data management standards for the data utilized in the preparation of ICAAP and fix accountability of data quality to respective departments which generate and manage the data.
- To provide periodic reports to the RMC on the following areas in a timely manner

    - Risk Profile Assessment
    - Capital Planning
    - Results of Stress Testing

6.4 Roles & Responsibilities of the Chief Risk Officer (CRO)

The Chief Risk Officer (CRO) is a senior executive responsible for administering an organization's risk management program. The specific responsibilities of a CRO can vary subject to the industry. company size, and organizational structure, but a few general responsibilities of a CRO include:

- Build and Implement the Risk Management Strategy: The CRO is in charge for developing and implementing the organization's risk management strategy, which incorporates the recognition of prospective risks and emerging plans to abate them.
- Risk Assessment and Monitoring: The CRO is responsible for evaluating and supervising the organization's exposure to various types of risks, such as financial, operational, legal, and reputational risks. This encompasses identification of potential risks, examining their impact, and observing modifications in the risk background.
- Compliance: The CRO is in control for ensuring that the organization conforms with relevant laws, regulations, and internal policies linked to risk management. This comprises of ensuring that the organization has ample controls and procedures in place to supervise risk and that employees are guided to follow these controls and procedures.
- Predicament Management: The CRO is liable for developing and implementing plans to supervise crises, such as natural disasters, cyber-attacks, and other unforeseen events that could have a visible impact on the organization.
- Reporting: The CRO is responsible for sharing regular reports to senior management and the board of directors on the organization's risk profile, including potential risks, risk mitigation strategies, and any variations in the risk environment.
- Stakeholder Engagement: The CRO is accountable for engaging with stakeholders, which comprises of investors, regulators, customers, and employees, to communicate the organization's risk management strategy and offer assurance that the organization is effectually dealing with risks.

Overall, the CRO plays a crucial role in aiding organizations to recognize and handle risks in order to push their strategic objectives while maintaining compliance with laws and regulation.

7. Risk Management Process

The risk management process is a framework for the actions that need to be taken. Implementing a risk management process is vital for any organization. With any new project comes new risks lying in it. MCSL following these below risk management steps to streamline the team for success, making the team more agile and responsive when risks do arise. MCSL follows the standard process to governance the organization risk. Identifying, Analyzing, Evaluating, Treating and Monitoring the risks above is vital for an organization, detailed discussion of which is followed ahead.

7.1 Identify the risk.

Anticipating possible pitfalls of a project doesn't have to feel like gloom and doom for the organization in fact, identifying risks is a positive experience that your whole team can take part in and learn frons. There are several types of risk few of which are mentioned below. The detailed description of the following types of risks are in the section ahead.

- ✓ Credit Risk
- ✓ Operational Risk
- ✓ Compliance Risk
- ✓ Reputational risk
- ✓ Strategical Risk
- ✓ Liquidity Risks
- ✓ Capital/Leverage Risk
- ✓ Information and Security Risks
- ✓ Securitization Risk and Off-Balance sheet Risk
- ✓ Climate Change Risk
- ✓ Political Risk
- ✓ Environment, Social and Governance Risk
- ✓ Vendor Management Risk

It is important to identify as many of these risk factors as possible in a manual environment, these risks are noted down manually. In order to identify the risks associated to various departments, the risk management team performs the RCSA periodically, with each stakeholder. This approach offers a detailed review of departmental risk to each stakeholder and top management of the organization. Apart from this, the company's data is extracted, and the relevant variables are chosen for covering the aforementioned risk types. The report must be shared with all the departmental heads, top management, and other required members for their visibility.

7.2 Analyze the Risk

While some risks can be modest in nature, some of the risks can bring the business to a standstill. Irrespective of the risk's nature, it needs to be analyzed in order to understand the link between the risk and different factors within the organization. To determine the severity and seriousness of the risk it is necessary to keep a check on the various business functions that are affected by risk.

Based on the RCSA report the risk management team further analyses the risks associated department. If required, the team will discuss mapped risks as per policies, procedures, and the processes with the respective SPOC of respective department.

7:3 Evaluate the Risk

Ranking and prioritizing risks is of utmost importance for a business. A risk that may cause inconvenience is rated low whereas, risks that can result in catastrophic loss are rated the highest. Ranking of risks should be performed in a responsible manner because it allows the organization to gain a holistic view of the risk exposure to the whole organization: The business may be susceptible to several low-level risks, but it may not require upper management intervention. On the other hand, just one of the highest-rated risks is enough to require immediate intervention.

MCSL risk management team will evaluate the risks individually for every department individually based on the different factors affecting them.

The components are classified into five categories mentioned below:

- Very High
- High
- Moderate
- Low
- Very Low

The risk management team will do prioritization of all risk based on the severity and risk score after evaluating. The result will be shared to all department heads and top management for their visibility and on time action.

7.4 Treat the Risk

Treating risk focuses on the risks that need to be eliminated or contained as much as possible. The risk treatment, the organization categorizes all the risks in the buckets that follow:

- Risk Reduction
- Risk Sharing
- Risk Transfer
- Risk Acceptance
- Risk Avoidance (Not recommending)

Risk treatment is done by connecting with the experts of the field to which the risk belongs. MCSL management team contacts each stakeholder and then sets up meetings in order to brainstorm through the issues. The team comprises of the risk team members, department expert, department heads and the top management (if required). The team will discuss and find the solution for the risks, if the solution in unavailable, then mitigation steps are found and finally the list of risks needed to send for acceptance from management is passed along.

7.5 Monitor and Review the Risk

Not all risks can be eliminated, some risks are always present. Market risks and environmental risks are just two examples of risks that require consistent monitoring. Under manual systems, monitoring happens through diligent employees. These professionals must ensure that they keep a close look on all the risk factors. The risk management team shall conduct several surveys, analysis (dump analysis, vulnerability scans, fraud analysis, etc.) to monitor the residual risk factors. The team will always have an eye of future risks by analyzing the different aspects of the same.

8. MCSL Risk Structure

It is recommended that the risks faced by an organization should be in-sync to what the organization does. There are numerous categories which are considered while grouping risks according to the various aspects of the organization. It ensures that the users can track the origin of the underlying and potential risks faced by an organization. These categories help determine the efficiency of the control systems implemented in all the departments of an organization. MCSL has six major categories of risk and not-categorized risk are included in Other Risk. The following are the details of risk categorized in MCSL.

8.1 Credit Risk

Credit Risk for the Company is the risk of loss of interest income and the Company's inability to recover the principal amount of the loan disbursed to its customers.

This risk can result from:

- Lack of appropriate tools to identify and control portfolio risks.
- Lack of control on hygiene factors like post disbursal documents.
- Information asymmetry and excessive reliance on Credit Bureau check, not backed by soft information or market intelligence of borrowers, leading to adverse selection of borrowers.
- Default due to over-indebtedness.
- A volatile political presence in a region of exposure.

MITIGATION:

The first step in effective credit risk management is to gain a complete understanding of overall credit risk by viewing risk at individual, customer, and portfolio levels. The mitigation plan aims to address the three aspects comprehensively.

Location Selection

Before establishing any branch, the following aspects shall be analyzed by the senior management.

- Potential for the business;
- Delinquency Risk - to see the history of inherent history of high delinquency, and if the

same is localized.

- Negative areas in the location.

This mitigates the risk of operating in highly delinquent areas. Separately, a feedback mechanism is incorporated in terms of updating the negative area list from time to time (Annually).

Credit Bureau Check

A credit check is to be done for every customer through an automated system-to-system integration with the Credit Bureau. As part of this check, the following parameters are looked at to verify a customer's creditworthiness and also ensure that they are not overburdened.

- Default history
- Indebtedness

These will be dynamic and reviewed periodically based on RBI Regulations and our internal norms.

Multi-Step Customer Verification

The Company has established separate customer relationships (through Customer Service Executives who sources the loan and Welcome Calling) through tele callers who verified the authenticity.

The Company may introduce E-KYC which would mitigate the risk of impersonation.

Hygiene Dashboard

The Company to have process of developing trigger-based mechanism to address hygiene issues such as collection of post disbursal documents like insurance, invoice, and RC etc.

Early Warning System

The Company is envisaging to have an analytical model to identify and address delinquency trends and thereby pre-empting the default.

PD-LGD Models

The Company may develop analytical build for portfolio risk identification. Probability of Default (PD), Loss Given Default (LGD) models are expected to enhance the credit risk measurements.

Portfolio Management

Traditionally, companies have focused on monitoring of individual credits to take care of the overall credit risk. While this focus is important, it is also important to have in place a system for monitoring the overall composition and quality of various credit portfolios and investments. To start with, a simple portfolio

monitoring framework may be put in place to focus on the credit and investment portfolio from the following perspectives.

- Delinquency Bucket wise
- Geography wise

MCSL can manage the risk return trade off proactively by adopting portfolio approach to credit risk management. Sophisticated and scientific portfolio management for tracking of asset correlations and concentration requires statistical models to be put in place and upgradation of risk management/MIS/IT capabilities.

Concentration Risk

The company has taken the approach of the Herfindahl-Hirschman index (HHI) to understand and analyze its risk as per the geographic concentration.

The company is engaged with in-depth analysis which includes analyses such as state wise breakup of the AUM, etc. to keep a track of the trend in a timely fashion. Furthermore, natural calamities are also tracked for each state on a pan India level. The company also monitors the location wise concentration of credit risk.

8.2 Operational Risk

Operational Risk is the risk of possible losses, resulting from inadequate or failed internal processes, people and systems or from external events, which includes legal risks but excludes strategic and reputation risk. The risk can emanate from:

- Procedural lapses arising due to higher volumes of transactions
- Lapses in compliance with established norms; regulatory as well as internal guidelines
- Misplaced/lost documents, collusion and fraud
- Breakdown or non-availability of core business applications.

Skill gap and sudden attrition of key personnel in the organization, is also an operational risk, which needs to be countered and addressed by the application of appropriate HR strategies.

Operational Risk Management

MCSL must identify and assess the Operational Risk inherent in all material products, activities, processes and systems. It should also monitor that before new products, activities, processes, and systems are introduced, the Operational Risk inherent in them is adequately assessed.

MCSL along with new products / process assessments would primarily use the Risk and Control Self-Assessment (RCSA) to identify, evaluate, monitor, and mitigate key operational Risks within MCSL. Conducting the RCSA will help MCSL to achieve below goals.

- Identify key Operational Risks across various products and processes within MCSL.
- Assess the risks that matter in various business, products and processes.
- Assess the design and the effectiveness of internal controls.
- Prioritize the control improvement initiatives to manage the Operational Risk profile of MCSL.
- Develop (more effective) alternative controls for the unacceptable risks; and

- Assist in embedding Operational Risk Management process in day-to-day activities of MCSL.

The tracking of individual internal incidents data is an essential pre-requisite to the development and functioning of a robust Operational Risk Measurement System (ORMS). The losses and its analysis provide Insight to the quantum of Operational Risk faced by MCSL. The collection of loss data is not the goal of this exercise, the objective is to understand what went wrong'. Therefore, for each significant incident a root cause and lessons learnt analysis should be drafted by the risk management department.

MITIGATION:

Automation of Processes

In line with the Company's objective to automate the processes thereby minimizing errors and strengthening the due-diligence mechanisms, the Company shall undertake digitalization initiatives at par with best of industry standards.

Process Compliance

The Company shall have Process Compliance Team (comprising of RFCU/ Credit Team/Concurrent Audit) which carries out checks on locations and identifies gaps, and rolls out initiatives to correct loopholes. This is done primarily to:

- Ensure that the designed processes are being followed on the field – including interaction with the customers during various stages of the relationship lifecycle.
- Ensure all branch activities are carried out as per norms/procedures.
- Identify any process lapses/deviations and provide guidance to branches/employees to ensure compliance.

The Process Compliance Team submits their major findings to the Operational Risk Management Committee. This ensures that risks arising out of process lapses are mitigated.

Document Movement, Storage and Retrieval:

The Company recognizes the need for proper movement of document, storage of documents, and also their retrieval for audit and statutory requirements. The Company have put in place:

- **Physical Storage:** The Company shall keep all the physical loan documents stored in a specialized secure facility. The process may also be outsourced.
- **Scanned Copies:** The Company may store the scanned copies of the loan documents for easy retrieval especially for audit purposes where physical documents are not required.

Non-Compliance Reporting Policy

The Company encourages all its employees to report any non-compliance of the stated Company processes or policies without fear as. MCSL has a formal "Whistle Blower policy" that details the manner in which such issues are handled.

All issues reported are categorized for nature and severity:

- Financial or non-financial

- Major or minor
- Procedural lapse or gross violation
- Breach in process or disciplinary issue
- Monetary malpractice of violation of Code of Conduct

The Compliance Manager maintains a record of all the entire case history which is signed off by senior management on closure.

Internal Audits:

Internal Audit of the Company is to be carried out in accordance with the Audit Policy of the Company. The scope of this Internal Audit shall cover risk management (including fraud risk) and control monitoring review and advisory services, reviews of operational and financial processes and controls, documentation of various important processes and events, information technology reviews, governance and assurance reviews, operational compliance audits, verification on adherence to regulatory requirements and other ad hoc advisory or consulting services. The scope of these audits are reviewed periodically and modified to keep pace with a dynamic business environment. The Internal Audit is to be conducted with regular periodicity by an external firm and report on the same submitted to the Audit Committee after discussion and noting of comments of the Management.

The Company also envisages to put in place an effective online fraud management system (analytics based) to highlight anomalies and abnormal transactions to take pre-emptive/proactive steps to identify, verify, and prevent such instances.

Technology Infrastructure:

The business applications in the Company (in-house) are hosted in secure data centers such that in the event of any system going down, an alternate system is made operational within hours. The Company also leveraged cloud-based technologies for its systems.

The Company is also in the process of complying with Master Direction on IT framework & IT outsourcing norms prescribed by RBI. Business continuity process and disaster recovery modalities will be adhered to as per the guidelines. Detailed IT framework will be covered through IS Policy & IT Policy.

8.3 Compliance Risk

The Company is present in an industry where the Company has to ensure compliance with regulatory and statutory requirements. Non-compliance with the applicable laws and regulations would result in legal actions and penalties from the regulatory and/or statutory authorities, material financial loss and loss of reputation of the Company. Compliance risks includes but not limited to the following:

- Non-compliance with RBI directions and/or regulations
- Non-compliance with various statutory enactments and/or regulations
- Non-compliance with internal code, policies and procedures
- Non-compliance with covenants laid down by lenders

MITIGATION:

Compliance Risk mitigation is the process of developing and implementing controls such as standards, policies, procedures and guidelines to prevent or minimize compliance risks. Even though there are some inherent compliance risks of doing business, the Company is keen on monitoring such risks and mitigating the same. The process of mitigation includes the following:

a) Checklist on statutory compliance circulated to concerned departments and the compliance reports obtained on a quarterly basis.
b) Audit Committee and Board reviews status of compliance of all the laws applicable to the Company on a quarterly basis.
c) Proactively monitors and identifies new and changes in the relevant laws, regulations, circulars, notifications, etc. and reported to the concerned departments for compliance.
d) Reviews compliance related policies issued by the Company and determine whether additional or different obligations, regulations or standards apply.
e) Resolves conflict between policies issued by the Company and various statutory enactments and/or regulations from time to time.

8.4 Reputation Risk

Reputation Risk is the risk to earnings and capital arising from adverse perception of the image of the company, on the part of customers, counterparties, shareholders, investors and regulators. It refers to the potential adverse effects, which can arise from the Company's reputation getting tarnished due to factors such as unethical practices, regulatory actions, customer dissatisfaction and complaints leading to negative publicity. Reputational risk can be a matter of corporate trust.

This risk can emanate from:

- Non-compliance with regulations
- Customer dissatisfaction

MITIGATION:

- **Strict adherence to Fair Practice Code:** The Fair Practice Code sets out the minimum practices to be followed by the Company while dealing with the customers. It aims to provide the necessary information to the customers and to increase the transparency which will enable the customers to take informative decisions and to appraise them of the services rendered by the Company. All the employees of the Company are instructed to follow fair practices in all their dealings to promote a fair and cordial relationship with the customers.
- **Grievance Redressal Mechanism:** As part of the Fair Practice Code, the Company has in place, a well-defined Grievance Redressal Mechanism. The Grievance Redressal Mechanism is displayed at all the Branches and is available on the website of the Company. The same including toll-free number is communicated to all customers.
- **Customer Connect:** The Company has established a call center to proactively reach out to its customers to ensure service quality and adherence to Company policies/processes by the field employees.

- **Delinquency Management**: The Company shall not resort to any coercive recovery practices and has an approved delinquency management process including specific Do's and Don'ts.

8.5 Strategic Risk

Strategic Risk is the risk to earnings and capital arising from lack of responsiveness to changes in the business environment and/or adverse business decisions, besides adoption of wrong strategies and choices.

MITIGATION:

This is being addressed and the risk mitigated to a great extent by referring matters of strategic importance to the Board, consisting of members with diversified experience in the respective fields, for intense deliberations, so as to derive the benefit of collective wisdom.

MCSL must keep in check, various factors which play a major role in monitoring strategic risk. Factors which MCSL must cover are the changes in its competitive environment, Regulatory environment, Technology changes, Product profiling, Business planning and Strategic Planning. The factors mentioned above include how well the company is adapting to new technology, pace of product diversification, pace of adapting to regulatory changes, resilience to competitor's changes, smooth budget allocation, governance, and involvement of the board.

8.6 Liquidity Risk

Liquidity Risk arises largely due to maturity mismatch associated with assets and liabilities of the Company. Liquidity risk stems from the inability of the Company to fund increase in assets, manage unplanned changes in funding sources and meet financial commitments when required.

Due to the reliance on external sources of funds, the Company is exposed to various funding and liquidity risks comprising:

- **Asset-Liability Mismatch**: A skewed asset-liability profile can lead to severe liquidity shortfall and result in significantly higher costs of funds, especially so during times of crises.
- **Interest Rate Risk**: Interest Rate Risk comprises the risk of increase in cost of funds due to an overall increase in the interest rates economy as well as sharp movements in interest rates across maturity profiles of the liabilities.

The management of interest rate and liquidity risks shall be articulated in the Liquidity risk Policy.

8.7 Capital and Leverage Risk

A high degree of leverage can severely impact the liquidity profile of the Company and lead to default in meeting its liabilities. Compliance of covenants of lenders and any operational delays in repayment of loans may have impact in the liquidity of the company.

This risk can emanate from:

- Non-compliance with sanction terms
- Delay in repayments
- High borrowings

MITIGATION:

- Strict adherence to sanction terms
- Prompt repayment of loans
- Monitoring of leverage ratio regularly

8.8 Information Technology Risk

IT risks include hardware and software failure, human error, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods.

Risk assessment includes.

- understand and identify the types of IT risks.
- understand the impact of risks on business.
- manage risks using policies and procedures.
- conduct regular staff training to further lower risk from potential threats.

A comprehensive risk assessment of IT systems to be done on a yearly basis. The assessment should make an analysis on the threats and vulnerabilities to the information technology assets and its existing security controls and processes. The outcome of the exercise should be to find out the risks present and to determine the appropriate level of controls necessary for appropriate mitigation of risks. The risk assessment should be brought to the notice of the Chief Risk Officer (CRO), CISO, CIO and the Board.

Information Security Assessment is a formal and recurring method for identifying the information security risks being faced by the organization. The purpose of this Information Security is to control access to sensitive information, ensuring use only by legitimate users so that data cannot be compromised or read without proper authorization.

The basic tenets of the IS Policy are as follows:

- Confidentiality – Ensuring access to sensitive data to authorized users only.
- Integrity – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization.
- Availability – Ensuring that uninterrupted data is available to users when it is needed.

- Authenticity – For IS it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

IT governance is already defined in the IT & Information Security Risk Management Policy of the company. IT risk management procedures are annexed to IT & Information Security Risk Management policy and Information Security policy, IT outsourcing policy, Cyber Security Policy, Outsourcing of Financial Services Policy, and Business Continuity Policy would be adhered to.

IT Risk Management Strategy

Strategy depends on the scope, nature, company structure, complexity, resource availability, and team capabilities. MCSL IT risk management process has been developed together by the risk management and IT team. For a better insight of all the risks the organization is exposed to, both teams work collectively to understand the future. There are numerous validations like RCSA, internal audits, stringent assessment which have been conducted for spotting the fields threatened by the lack of IT security.

MCSL conducts IT audit once a year to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity, and availability of the organization's IT infrastructure.

8.8.1 IT Services Outsourcing Risks

"Outsourcing may be defined as use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by itself, now or in the future. In the event of certain IT services being outsourced MCSL is exposed to various types of Risk. It is imperative that MCSL implement necessary controls and risk management measures to ensure that the risks are manageable.
MCSL shall ensure that the outsourcing shall neither impede nor interfere with the ability to effectively oversee and manage its activities. Even if MCSL outsources some of the IT related activities, the responsibility for redressal of customers' grievances related to outsourced services shall rest with MCSL.

8.8.2 Information Security Risks

Information security risk comprises the impacts to an organization and its stakeholders that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate. The primary means of mitigating information security-related risk is through the selection, implementation, maintenance, and continuous monitoring of preventive, detective, and corrective security controls to protect information assets from compromise or to limit the damage to the organization should a compromise occur. Information security risk overlaps with many other types of risk in terms of the kinds of impact that might result from the occurrence of a security-related incident. It is also influenced by factors attributed to other categories of risk, including strategic, budgetary, program management, investment, political, legal, reputation, supply chain, and compliance risk.

8.8.3 Cyber Security Risk

Network security is the most important aspect of keeping your data safe and secure. It involves encryption and other security measures to protect one's data from being accessed by unauthorized people.

Cyber security is the activity which involves safeguarding of networks, computer systems, devices, and applications from cyber-attacks of numerous kinds. Cyber security threats have soared above critical levels

because of the inevitable spread of digital transformation, putting the organization's sensitive data in extreme trouble.

MCSL shall taken all necessary steps to protect information and information infrastructure in internet/cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation from relevant external bodies both Private, Public and the Government.

MCSL has a Cyber security policy applicable to all cyber facing Information/ Data/ Information Processing facilities and IT assets of the Organization which is available to or accessible by the organization, employees, vendors, contractors, consultants, temporary staff and other individuals even if, affiliated with Third Parties and are utilizing the Organization's network. All automated information assets and services that are utilized by the Company's Network are covered by this policy. The objective of this Policy is to proactively identify the Cyber threats and the risks manifested in information infrastructure and manage, mitigate, avoid, transfer or accept the risks as per the risk appetite of the organization.

8.8.4 Outsourcing of Financial Services Risk

'Outsourcing' is defined as the NBFC's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the Company, now or in the future. It includes agreements for outsourcing for a limited period also.

Typically, outsourced financial services include application processing (loan origination, credit card etc.), document processing, marketing and research, supervision of loans, data processing and back office related activities, besides others. However, they relate to technology-related issues and activities not related to financial services, such as usage of courier, catering of staff, housekeeping and janitorial services, security of the premises, movement and archiving of records, etc.

Activities identified as eligible for outsourcing by the Company as an outsourcer as follows:

Sl. No.	**Activities outsourced**
1	Customer Profile Verification
2	Processing of customer files/documents
3	NACH processing/presentations
4	Collections of customer dues
5	Sourcing of public deposits
6	Financial fund arrangers
7	Data server
8	Sales & Collection services
9	Field investigation

8.8.5 Third Party arrangements Risk

Third-Party Risk is any risk associated with engaging a third party in the context of providing a service or product to a client (the second party). It is an umbrella term covering several potential risk types depending on the product or service, the third party and the nature of the engagement / relationship.

Potential Risks due to Third-Party Risk

There are numerous risks that may arise from a financial institution's use of third parties[1]

Some of the risks are associated with the underlying activity itself, similar to the risks faced by an institution directly conducting the activity. Other potential risks arise from or are heightened by the involvement of a third party. Failure to manage these risks can expose an institution to regulatory action, financial loss, litigation and reputation damage, and may even impair the institution's ability to establish new or service existing customer relationships.

- Reputation Risk. Reputation risk is the risk arising from negative public opinion. Third-party relationships that result in dissatisfied customers, interactions not consistent with institution policies, inappropriate recommendations, security breaches resulting in the disclosure of customer information, and violations of law and regulation are all examples that could harm the reputation and standing of the financial institution in the community it serves. Any negative publicity involving the third party, whether or not the publicity is related to the institution's use of the third party, could result in reputation risk
- Operational Risk. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. Third-party relationships often integrate the internal processes of other organizations with the bank's processes and can increase the overall operational complexity
- Transaction risk. Transaction risk a form of operational risk (Business Execution). It is the risk arising from problems with service or product delivery. A third party's failure to perform as expected by customers or the financial institution due to reasons such as inadequate capacity, technological failure, human error, or fraud, exposes the institution to transaction risk. The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk. Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources. These issues could result in unauthorized transactions or the inability to transact business as expected
- Credit Risk. Credit risk is the risk that a third party, or any other creditor necessary to the third-party relationship, is unable to meet the terms of the contractual arrangements with the financial institution or to otherwise financially perform as agreed. The basic form of credit risk involves the financial condition of the third party itself. Some contracts provide that the third party ensures some measure of performance related to obligations arising from the relationship, such as loan origination programs. In these circumstances, the financial condition of the third party is a factor in assessing credit risk. Credit risk also arises from the use of third parties that market or originate certain types of loans, solicit and refer customers, conduct underwriting analysis, or set up product programs for the financial institution. Appropriate monitoring of the activity of the third party is necessary to ensure that credit risk is understood and remains within board-approved limits
- Compliance risk. Compliance risk (Legal Risk) is the risk arising from violations of laws, rules, or regulations, or from non-compliance with internal policies or procedures or with the institution's

business standards. This risk exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, policies, or ethical standards.

8.8.6 Business Continuity & Disaster Recovery Risk

Business continuity and disaster recovery, also known as BCDR, is a set of closely related practices that support an organization's ability to remain operational after an adverse event. Business Continuity Management is the overall management system that establishes implements, operates and monitors, reviews and maintains and improves business continuity. Business Continuity Management capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents. The organisation's ability and readiness to manage business interruptions are evaluated in order to provide continuity of services at a minimum acceptable level and to safeguard the company's financial and competitive position in the short and the long term.

Business Continuity: Focuses on maintaining overall business operations during various disruptions, from power outages to cyberattacks. It includes plans for critical functions, communication, and keeping the business running in some capacity, even if reduced.

Disaster Recovery: Deals specifically with recovering IT systems and data after a major disaster or crisis. This ensures critical applications and information are restored and accessible again.
DR is a subset of the overall business continuity.

8.9 Securitization Risk and Off-Balance sheet Risk

Securitisation Risk:

Securitisation has been used as an alternative source of funding and as a mechanism to transfer risk to investors. Securitisation involves transactions where credit risk in assets are redistributed by repackaging them into tradeable securities with different risk profiles which may give investors of various classes access to exposures which they otherwise might be unable to access directly.

The credit risk on securitised exposure is factored in Credit Risk analysis since under new accounting norms (Ind AS) securitized exposure becomes part of the on-balance sheet and is not derecognised. Further, the Credit enhancement towards the securitisation are deducted from Tier I and tier II capital under pillar. Interest rate risk, Liquidity risk and Reputational Risk of the securitised exposure have been considered in the respective risk assessment.

Off-balance sheet Risk is a risk related to the excessive growth rate in contingencies. There are mainly three types of off-balance risks.

1. Funding and Liquidity Risk: Off-balance sheet liquidity risk sources for the institution. These include items which may cause additional funding demands in the future:

- Undrawn lending facilities.
- Contingent liabilities e.g. guarantee.
- Securitization vehicles for special purposes.
- Derivative instruments.

2. Risks of negative effects on the capital and profits of company from similar off-balance sheet sources.
3. An organization's any risk arising from contingencies, relationship, or events not recorded in the balance sheet of the organization.

8.10 Other Risk

8.10.1 Climate Change Risk

As the globe experiences industrialization, climate change risk takes the top place in the list of risks being faced by the organization. UNDP, IPCC, OECD, WHO and several other important bodies have committed to climate action.

As för India, RBI has rolled out a discussion paper on Climate Risk and sustainable finance dated July 27, 2022, which encourages the companies to keep a check on the severity of climate change's impact on their portfolio.

MCSL takes care of the disbursement and collection status of each state by taking base reports published by credible agencies to understand and evaluate the risks involved with respect to climate change.

Wherever required, the portfolio would be analyzed by the Risk department and all the findings are presented to the committees of the senior management, where further action such as, covering insurance or limiting the disbursement in those districts.

8.10.2 Political Risk

Political risk is the threat that political actions or outcomes pose to corporate interests. Political risks can be either macro, affecting the entire nation, or micro, affecting only a specific sector, region, or organization.

Legitimate governments' actions, such as limitations on outputs, prices, and activities, as well as restrictions on foreign exchange and remittances, may result in political risk. Events that are not beyond the authority of the government, such as war, revolution, terrorism, labour strikes, regional influences, and extortion, can also cause political risk.

At the operational level, local politicians with vested interests spin any disturbance with financial repercussions, like COVID 19, policy initiatives, like demonetization, as potentially resulting in loan waivers and mislead trusting customers, India has seen numerous debt waivers; thus it is simple to attract the attention of the underprivileged.

MCSL has been facing issues due to stress from political parties in certain revenue States. The same can be avoided with the help of the regulatory authority, which can set up guidelines to lessen the effects of unforeseen political situations.

8.10.3 Environment, Social and Governance Risk

ESG stands for Environmental, Social, and Governance. Investors are increasingly applying these non-financial factors as part of their analysis process to identify material risks and growth opportunities. MCSL has dedicated a policy which talks about the concept of overall sustainable development, thereby dictating the organization to recognize Environmental and Social (E&S) considerations in its own business operations and in the activities carried out by the people and institutions associated with it. MCSL's ESG policy has

issued detailed guidelines which imparts information on the company's governance structure with regards to ESG guidelines adherence. The policy has a separate discussion section about measures dedicated towards E-waste reduction by the organization.

8.10.4 Vendor Management Risk

Vendor Risk Management (VRM) is the process of identifying, assessing and mitigating the risk associated with using third-party vendors or suppliers. VRM involves assessing the risks associated with each vendor, such as their financial stability, security practices, compliance with regulatory requirements, and their ability to deliver the required goods or services. This helps businesses to identify potential vulnerabilities in their supply chain and take appropriate steps to manage or mitigate those risks. MCSL extracts vendor services in the field of IT, Financial services, RCU and infrastructure.

MCSL has a policy which talks about outsourcing of financial services and its Risk Management. The policy outlines several instances which focus on the preliminary rules and regulations while dealing with any vendor for services. Furthermore, the Reserve Bank of India (RBI) has released guidelines on outsourcing of IT services.

Both the policies talk about the services for which the company is eligible to opt for vendor services. Post that, guidelines on material outsourcing have been discussed in detail. The policies lay down regulations about the activities which the company cannot outsource along with the outsourcing agreement. Both the policies focus on the role of governance for vendor service sourcing activities. For the risk management committee, the policies expect the department to ensure promising and constructive monitoring of all the outsourcing activities taking place in the organization.

9. Risk Governance

Governance :

Weak corporate governance is a common threat found in many company failures. A lack of proper oversight by the board of directors, inadequate protection for minority shareholders, and incentives at companies that promote excessive risk taking are just a few of the examples that can be problematic for a company. Poor corporate governance practices resulted in several high-profile accounting scandals and corporate bankruptcies over the past several decades and have been cited as significantly contributing to the 2008-2009 global financial crisis.

In response to these company failures, regulations have been introduced to promote stronger governance practices and protect clients and investors.

Furthermore, academics, policy makers, and other groups have published numerous works discussing the benefits of good corporate governance and identifying core corporate governance principles believed to be essential to ensuring sound growth of the company. Muthoot Capital Services Ltd. has ensured that corporate governance within the organization is well defined and is being followed by the stakeholders of the organization.

The board's risk oversight role may include, but is not limited to:

- **Reviewing, challenging, and concurring with management on:**

-Proposed strategy and risk appetite.

-Alignment of strategy and business objectives with the entity's stated mission, vision, and core values

-Significant business decisions including mergers acquisitions, capital allocations, funding, and dividend-related decisions

-Response to significant fluctuations in entity performance or the portfolio view of risk.

-Responses to instances of deviation from core values.

- **Approving management incentives and remuneration.**
- **Participating in investor and stakeholder relations.**

Risk Governance: Risk Governance Typically, the risk management department has co-jurisdiction over IRM. The risk management department is responsible for setting up the appropriate risk control mechanism, quantifying and monitoring risks, and responsible for allocating risk capital to business units after assessing return. Though it is the risk management department that is primarily responsible for IRM, it is also the responsibility of everyone within the organization, across levels and businesses. All decisions and actions of the management and employees should consider the risk perspective.

Key Responsibilities:

Independent Control Functions	**Key Responsibilities**
Board of Directors	Approve the risk appetite framework for the organization and discuss with executive management about prevailing risks
Executive Management	Define and monitor risk appetite statement Evaluate strategies/ action based on findings
Risk Management Department	• Create a common risk framework. • Provide direction on applying framework Implement and monitor risk management frameworks. • Define risk metrics and risk KPIs across all stakeholders. • Prevention of conflict of interest • Provide timely risk-related information
Business Units	• Identify and assess risks. • Monitors risk • Respond to risks

Internal Audit	• Independent review of effectiveness of the risk management practices. • Evaluate controls and risk response plans for significant risks and enforce corrective action where necessary

Risk management policies and procedures shall be developed using a top-down approach to ensure that they are consistent with one another and appropriately reflect the strategic objectives and the overall risk appetite of the institution. This means that corporate risk management policies and procedures are endorsed by senior management who shall actively work towards infusing them into the culture of MCSL. The risk management policies and procedures shall be applicable to all the products and services offered by MCSL, including existing as well as future products and services. Risk management policies and procedures shall provide detailed guidance on MCSL's risk management approach. They clearly communicate how the risk management infrastructure will work on a daily basis with respective roles, responsibilities and accountabilities towards risk management. Given the importance of policies and procedures it is critical that different departments within MCSL work collaboratively to develop them to ensure that they encompass all aspects of risk management.

Risk shall be managed through a pro-active approach which shall be built into the risk management process and shall be ensured through periodic reviews and reviews contingent of information made available towards setting risk limits, monitoring etc.

9.1 ICAAP Policy

The Reserve Bank of India (RBI) issued its Guidelines on Framework for Scale Based Regulation for Non-Banking Financial Companies. Scale Based Regulation framework encompasses different facets of regulation of NBFCs covering capital requirements, governance standards, prudential regulation. As per the framework, 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 . 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.
As per the requirements:

- Implement a process for assessing capital adequacy in relation to the company's risk profile as well as a strategy for maintaining adequate capital levels, known as Internal Capital Adequacy Assessment Process (ICAAP).
- Demonstrate that the chosen internal capital targets are well founded and that these targets are consistent with overall risk profile and current operating environment.
- Establish an adequate system for monitoring and reporting risk exposures and assessing how MCSL's changing risk profile affects the future need for capital.

- Document the methodologies, assumptions and procedures regarding capital policy and capital assessment process.
- Continuously operate within the target capital adequacy ratio and always above the minimum regulatory capital requirement.

ICAAP Management and Measurement into two separate activities.

Part A comprises of the ICAAP Policy i.e., the current document which contains the ICAAP Framework, ICAAP Governance, Roles and Responsibilities of various Departments involved in ICAAP implementation and management, high level discussion on methodologies and other procedures to be followed for ICAAP maintenance. Review of ICAAP Policy will be undertaken on an annual basis.

Part B comprises of the ICAAP Document, which contains the detailed notes and calculations as at end of year, in the areas of risk profile assessment, capital budgeting and stress testing.

MCSL shall ensure that detailed documentation of methodologies, assumptions, data inputs, procedures and minutes of meetings etc., are available for all the processes of ICAAP and are communicated to the concerned stakeholders and appropriate authority and responsibilities have been delegated. Risk Department will be the central department in this aspect coordinating between different departments within the company in implementation, maintenance, and management of ICAAP.

10. Risk Reporting

Enterprise Risk Management will not be completed without a structured process for reporting of risk related information, to all its stakeholders. Risk Reporting therefore has two significant categories, Reporting to External Stakeholders and Reporting to Internal Stakeholders.

10.1 Risk Reporting to External Stakeholders

External Stakeholders are always regulatory and legislative bodies. As a Financial institution, MCSL has to submit many reports to the regulators. The Compliance Department will interact with the Regulators, but it will also advise all internal stakeholders on the relevant and extant reporting to be followed, from time to time.

10.2 Risk Reporting to internal Stakeholders

Internal stakeholders are primarily following below

1. Board of Directors

2. Risk Management Committee

3. Top Management Team

4. Functional Management Teams

5. Operational Stakeholders

Thus, Risk Reports to Internal stakeholders can be classified as

- Strategic Reports on Risks: Reports that help formulate or review strategies.

- Tactical Report on Risks: Reports that help review the need for course corrections.
- Functional Reports on Risks: 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.

10.3 Reporting to the Board of Directors

Periodic Reporting to RMC: The CRO will submit a detailed summary on the overall Risk Status of the Company, based on the ERM Framework. This status report will be in the form of a dashboard, with relevant details.

11. Review of Framework :

The above framework shall be subject to annual review/changes by the RMC & Board as may be deemed necessary and in accordance with regulatory amendments, from time to time.