IndoStar Capital Finance Limited

Enterprise Risk Management Framework

FOR INTERNAL PURPOSE ONLY

April, 2024

Enterprise Risk Management Framework

Table of Contents

Enterprise Risk Management Framework

1. Introduction

IndoStar Capital Finance Limited (referred herein as “IndoStar” or “the NBFC” or “the company”) registered with the Reserve Bank of India as a Middle layered NBFC. With Brookfield & Everstone as co-promoters, IndoStar is a professionally managed and institutionally owned entity engaged in providing used and new commercial vehicle financing, structured term financing solutions to corporates, loans to SME borrowers, affordable Home Finance through its wholly owned subsidiary, IndoStar Home Finance Private Limited and such other products as it may plan to enter from time to time.

1.1. Background

Enterprise risk management (ERM) is defined as “the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value”.

Enterprise risk management is a process, effected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. The definition of enterprise risk management emphasizes its focus on managing risk through:

- Recognizing culture
- Developing capabilities
- Applying practices
- Integrating with strategy-setting and performance
- Managing risk to strategy and business objectives
- Linking to value

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

IndoStar has documented the enterprise risk management policy document to ensure that the overall risk taken on by the company does not exceed its risk-taking capacity and to identify and monitor the different types of risks faced by the company. This document details the concept, approach, governance, risk mitigation, monitoring and reporting practices to be followed by the company for compliance with its enterprise risk management framework.

1.2. Objectives

The objective of enterprise risk management policy document ("the policy") is to lay down the broad principles, guidelines and procedures governing the framework for risk identification, assessment, measurement and reporting process of the business risks. The policy aims to ensure that all material business risks can be identified and managed in a timely and structured manner.

The enterprise risk management policy serves as a cornerstone for achieving sustainable growth with profitability. The core objective is to ensure the Board of Directors and Senior Management remain promptly and regularly informed about all relevant risks. This policy framework safeguards the company's risk framework, risk appetite and reputation, empowers the Company to make consistently sound and profitable business decisions across all its offices, and fosters an environment that prioritizes achieving an overall organizational objectives.

Furthermore, the policy establishes a robust risk management framework built upon the foundation of clearly defined risk appetite, risk tolerances, and applicable risk limits. This framework ensures IndoStar operates within its overall risk capacity, allowing for balanced growth while adhering to responsible risk management practices. Ultimately, the policy empowers IndoStar to strive for a pre-eminent position amongst NBFCs by facilitating informed decision-making and fostering a culture of risk awareness throughout the organization.

2. Components and Principles of Enterprise Risk Management

The ERM Framework prescribed by Committee of Sponsoring Organizations of the Treadway Commission (COSO) consists of the five interrelated components of enterprise risk management. The five components are:

- **Governance and Culture:** Governance and culture together form a basis for all other components of enterprise risk management. Governance sets the entity's tone, reinforcing the importance of enterprise risk management, and establishing oversight responsibilities for it. Culture is reflected in decision-making.

- **Strategy and Objective-Setting:** Enterprise risk management is integrated into the entity's strategic plan through the process of setting strategy and business objectives. With an understanding of business context, the organization can gain insight into internal and external factors and their effect on risk. An organization sets its risk appetite in conjunction with strategy setting. The business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities.

- **Performance:** An organization identifies and assesses risks that may affect an entity's ability to achieve its strategy and business objectives. As part of that pursuit, the organization identifies and assesses risks that may affect the achievement of that strategy and business objectives. It prioritizes risks according to their severity and considering the entity's risk appetite. The organization then selects risk responses and monitors performance for change. In this way, it develops a portfolio view of the amount of risk the entity has assumed in the pursuit of its strategy and entity level business objectives.

- **Review and Revision:** By reviewing enterprise risk management capabilities and practices, and the entity's performance relative to its targets, an organization can consider how well the enterprise risk management capabilities and practices have increased value over time and will continue to drive value in light of substantial changes.

- **Information, Communication, and Reporting:** Communication is the continual, iterative process of obtaining information and sharing it throughout the entity. Management uses relevant information from both internal and external sources to support enterprise risk management. The organization leverages information systems to capture, process, and

manage data and information. By using information that applies to all components, the organization reports on risk, culture, and performance.

3. Risk Management Approach

IndoStar prioritizes safeguarding its future through a robust enterprise risk management framework aligned with industry best practices. This framework employs a proactive approach to identify potential threats. It actively seeks out risks through industry analysis, scenario planning, employee input, and benchmarking against successful NBFCs. Once identified, each risk is meticulously assessed based on its likelihood of occurrence (probability) and potential impact (level of impact and criticality) on financial performance, operations, reputation, and regulatory compliance. A severity score is then assigned to prioritize risks and allocate resources for mitigation efforts.

The company adopts a tailored approach to address each risk. Wherever possible, it eliminates the threat entirely, such as diversifying funding sources or investing in cybersecurity. For unavoidable risks, it implements mitigation strategies like setting risk limits, developing contingency plans, and strengthening internal controls. In some cases, it may transfer the risk burden through insurance or outsourcing services. Finally, for low-probability or low-impact risks, it may choose calculated acceptance with close monitoring and mitigation plans in place.

This policy extends beyond identification and assessment. The findings guide the creation of a comprehensive risk management framework outlining specific actions and controls for each chosen risk treatment strategy. The company embeds its risk management considerations into its processes and systems for ongoing mitigation and reduction. Recognizing the ever-changing risk landscape, the company shall continuously evaluate the ERM process and identified risks to ensure that the ERM framework remains relevant and adaptable. The commitment to continuous improvement shall empower the company to stay ahead of potential threats while identifying and capitalizing on emerging opportunities, ultimately safeguarding its success and ensuring long-term sustainable growth.

4. Risk Management Framework

The company understands the critical role of a robust risk management framework in realizing its business objectives. The ERM framework prioritizes proactive identification and analysis of potential risks. The company evaluates each risk's likelihood and potential impact to determine the most suitable response strategy, which may involve risk elimination, mitigation, transfer, or acceptance within established tolerances.

To ensure the effective execution of this framework, IndoStar has instituted dedicated committees with distinct focuses:

Board level committees:

- **Risk Management Committee (RMC):** Offers overarching guidance and direction for risk management practices
- **Credit Committee (CC):** Oversees credit risks associated with lending activities
- **Asset Liability Management Committee (ALCO):** Supervises the management of assets and liabilities to maintain a balanced risk profile
- **IT Strategy Committee:** Addresses IT-related risks through cybersecurity measures and business continuity plans
- **Grievances Redressal Committee:** Addresses complaints of borrowers or customers of the Company
- **Disciplinary Committee:** Addresses issues pertaining to adequacy and implementation of codes /policies of the Company

Senior management level committees:

- **Internal Complaints Committee:** Addresses complaints made by any aggrieved woman at the workplace and monitors and the Company's Care and Dignity Policy
- **ESG Working Committee:** Oversees and implements the Business Responsibility Policies as required under Business Responsibility and Sustainability Report (BRSR)
- **Outsourcing Committee:** Oversees the outsourcing risks faced by the company including functions to be outsourced, approval for outsourcing and regular review

This collaborative approach, with clearly defined roles and responsibilities, nurtures a culture of risk awareness across IndoStar. It equips us to navigate dynamic risk landscapes effectively and achieve sustainable growth.

5. Risk Governance and roles and responsibilities

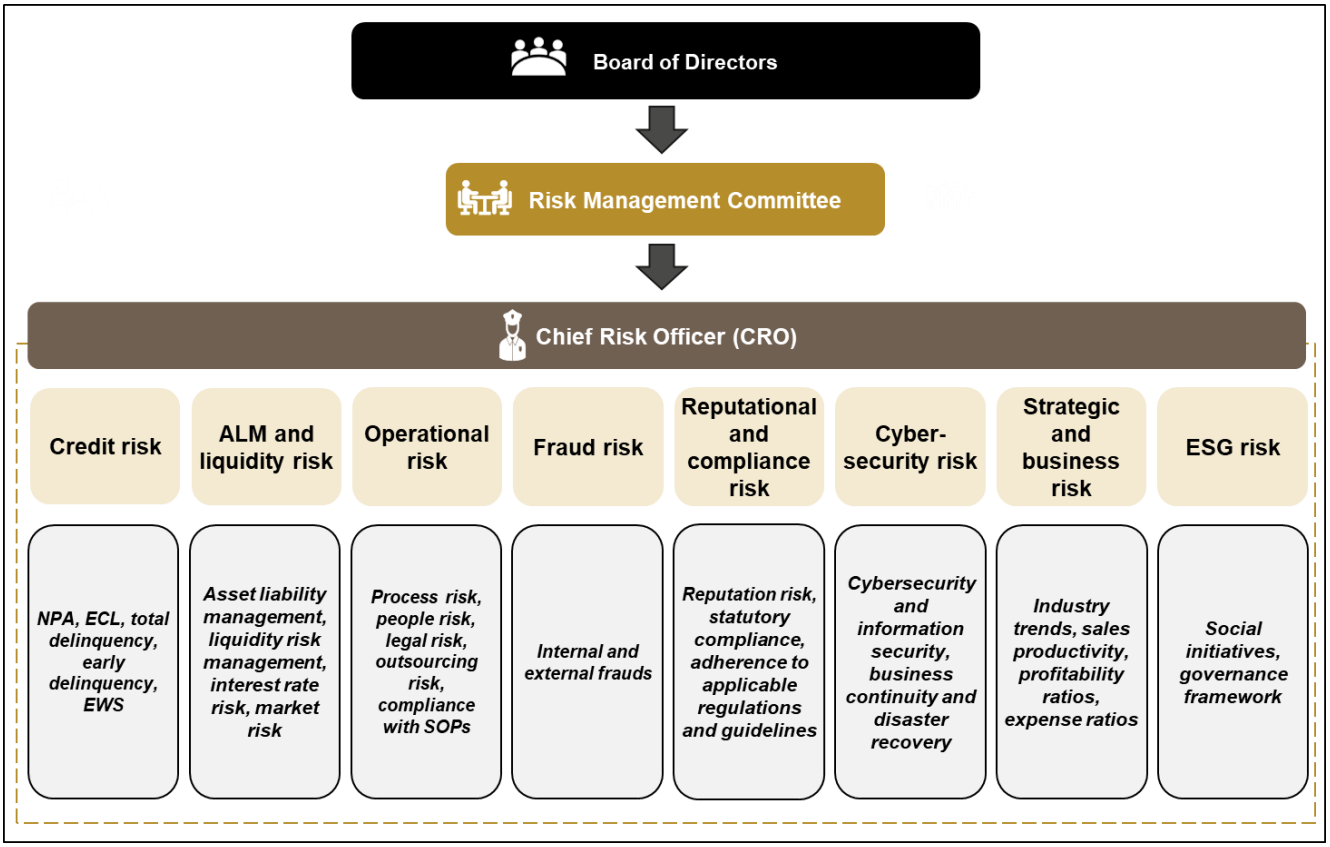
5.1. Guidelines and governance framework

The company's risk governance framework operates on a set of fundamental principles to ensure effective management of risks across the organization. The Board of Directors holds overall responsibility for governance and oversight of core risk management activities which delegates the execution strategy to the RMC. Segregation of duties follows the 'three lines of defence' model, ensuring independence between front-office functions, risk management & oversight, and internal audit roles.

Risk strategy, aligned with the company's risk appetite, is approved by the Board annually to align risk, capital, and performance targets. Major risk classes, including credit risk, market risk, operational risk, and liquidity risk, are managed through focused and specific risk management processes. As the company evolves in risk management sophistication, it will implement advanced risk management models suitable for the size, scale, and complexity of its business. Policies, processes, and systems are established to enhance the company's risk management capability. Additionally, monitoring, stress testing tools, and escalation processes are implemented to monitor performance against approved risk appetite.

The figure below exhibits a brief overview of the company's risk management framework:

Enterprise Risk Management Framework



5.2. Board of Directors

The Board of Directors is responsible for:

- Providing risk oversight of enterprise risk management culture, capabilities, and practices.
- Delegating oversight authority to the RMC and operational authority to the Chief Risk Officer (CRO).
- Delegating approval authority for specific instances and for changes in the policies and procedural matters to the RMC.

5.3. Risk Management Committee

The RMC is the primary body responsible for managing risks within the organization. The membership, meeting frequency, terms of reference, quorum, etc. of the RMC shall be guided by the RMC Charter adopted by the company. The RMC oversees the risk management function of the company and approves various policies and processes related to risk management. The RMC is also responsible for:

- Reviewing the Company's risk appetite framework and recommending approval to the Board at least annually.
- Reviewing and considering for approval, the Company's Enterprise Risk Management Framework at least annually.
- Ensuring an appropriate risk organization structure with clearly defined authority and responsibility, and independence of Risk Management functions.
- Reviewing reports from management concerning the company's risk management framework.
- Providing timely and appropriate reporting to the Board of Directors to fulfill their oversight responsibilities.
- Reviewing reports from management concerning implications of new and emerging risks, legislative or regulatory initiatives, organizational changes, and major initiatives to monitor them.
- Reviewing the appointment, removal and terms of remuneration of the Chief Risk Officer
- Sub-delegating powers and discretions to executives of the company, with or without further power to delegate.
- Monitoring and reviewing non-compliance, limit breaches, audit/regulatory findings, and policy exceptions related to risk management.

- Ensuring appropriate methodology, processes, and systems are in place to monitor and evaluate all the risks that the company is exposed to.
- Monitoring and overseeing implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- Coordinating its activities with other committees as per the framework laid down by the Board of Directors.

5.4. Chief Executive Officer

The Chief Executive Officer (CEO) is accountable to the Board of Directors and is responsible for overall enterprise risk management culture, capabilities, and practices required to achieve the entity's strategy and business objectives. The CEO sets the tone at the top along with the explicit and implicit values, behaviors, and norms that define the culture of the entity. The CEO's responsibilities relating to enterprise risk management include:

- Providing leadership and direction to senior members of management, and shaping the entity's core values, standards, expectations of competence, organizational structure, and accountability.
- Evaluating alternative strategies, choosing a strategy, and setting business objectives that consider supporting assumptions relating to business context, resources, and capabilities within the risk appetite of the entity.
- Maintaining oversight of the risks facing the entity (e.g., directing all management and other personnel to proactively identify, assess, prioritize, respond to, and report risks that may impede the ability to achieve the strategy and business objectives).
- Guiding the development and performance of the enterprise risk management process across the entity and delegating to various levels of management at different levels of the entity.
- Communicating expectations (e.g., integrity, competence, key policies) and information requirements (e.g., the type of planning and reporting systems the entity will use).

5.5. Chief Risk Officer

The Chief Risk Officer (CRO) holds a pivotal role in overseeing risk management within the organization. This position is tasked with overseeing enterprise risk management as a second line of accountability. The CRO will be responsible for:

- Establishing ongoing enterprise risk management practices suitable for the entity's needs.

- Overseeing enterprise risk management ownership within the respective lines of accountability.
- Reviewing the operation of enterprise risk management in each operating unit.
- Promoting enterprise risk management to the operating unit leaders and assisting in integrating practices into their business plans and reporting.
- Identifying potential risk points within the organization and assessing or measuring their impact on business operations.
- Formulating risk management policies, ensuring that they are aligned with the organization's objectives and regulatory requirements.
- Devising strategies for controlling and mitigating risks, developing measures to minimize their impact on the organization's operations and objectives.
- Evolving organizational capabilities in line with the maturity and suitability of enterprise risk management.
- Reporting on risk matters to the Board, RMC and senior management, providing insights into the organization's risk profile and strategies for managing them effectively, discussing severe risks and emerging risks.
- Escalating identified or emerging risk exposures to executive management and the board.
- Vetting Operational Guidelines from a risk perspective, minimizing operational risks that could impact the organization's objectives.
- Participating in various committees, including RMC, ALCO, Management Committee, Borrowing Committee, Banking Committee, Corporate Committee, Retail Lending Committee and Disciplinary Committee.

5.6. Risk Management teams

The risk management teams act as a support function to the RMC, to other risk committees and to the CRO as a second line of defence. The risk management teams shall be responsible for the following activities to ensure effective implementation of the enterprise risk management framework:

- Designing the overall risk management framework, policies, and guidelines and ensuring that these are duly reviewed so as to align with latest regulatory landscape and industry best practices.
- Supporting management policies, defining roles and responsibilities, and setting targets for implementation.
- Providing enterprise risk management guidance.
- Supporting management to identify trends and emerging risks.

- Assisting management in developing processes and risk responses to manage risks and issues.
- Providing guidance and training on enterprise risk management processes.
- Monitoring the adequacy and effectiveness of risk responses, accuracy, and completeness of reporting, and timely remediation of deficiencies.
- Reviewing and monitoring the risk management processes of the first line of defence from an adequacy perspective.
- Maintains repository of all risk related activities in the organization.
- Responsible for overall awareness and risk culture in the organization.
- Providing risk MIS / reports on a regular basis.

5.7. Business and support functions

The first line of defence refers to the frontline functions within the company that directly engage in the day-to-day activities and operational processes. Both business and support functions play a crucial role in identifying and mitigating risks. The business and support functions are typically responsible for:

- Owning and managing the risks and implementing controls and safeguards directly within their operations.
- Conducting regular risk assessments and identifying risk incidents in their daily operations.
- Identifying mitigation strategies and ensuring timely implementation of the strategies.
- Providing periodic updates to the second line of defence on emerging risks.
- Implementing controls and safeguards directly within the operations.
- Implementing the day-to-day tasks to manage performance and risks taken to achieve strategy and business objectives.

Functional managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility consistent with risk appetite.

Other employees are responsible for executing enterprise risk management in accordance with established directives and responsibilities assigned and for reporting non-compliance, if any.

5.8. Internal Audit

A strong internal audit function is a fundamental element of a robust ERM framework. The internal audit function acts as the third line of defence in the company's risk framework thus providing independent assurance and oversight. By performing the following activities, internal audit plays a critical role in ensuring that the ERM program is functioning effectively and helping the organization achieve its risk management objectives. The internal audit function shall be responsible for:

- Reviewing and assessing the organization's enterprise risk management framework.
- Objectively evaluating the design and effectiveness of the ERM program.
- Assessing the risk identification and assessment processes i.e., whether all the relevant risks are being identified and accurately assessed.

- Assessing the risk mitigation controls i.e., whether appropriate controls are in place to manage identified risks.
- Evaluate the effectiveness of risk mitigation strategies.
- Reviewing the risk management practices within the departments on a regular basis and reporting as appropriate on issues arising from these reviews.
- Assessing the risk reporting and communication processes i.e., whether risk information is being communicated effectively and accurately across the organization.
- Independent and unbiased assessment of the ERM program to ensure it remains effective over time.
- Identifying areas for improvement within the ERM framework and recommending actions to strengthen the framework.
- Evaluating the design and operating effectiveness of the internal controls and identifying weaknesses, if any.
- Verifying that the company's risk taking activities are aligned with its risk appetite thus ensuring the organization is not taking on excessive risk.
- Assessing the integration of risk management into business planning and decision-making processes.
- Providing assurance to the Audit Committee of the Board with respect to effectiveness of controls over risks across the organization.

6. Credit Risk

Credit risk is defined as the possibility of losses associated with diminution in the credit quality of borrowers or counterparties. In the Company's portfolio, losses may stem from outright default due to inability or unwillingness of a customer or counterparty to meet commitments. The risk is that of the lender and includes lost principal and interest, disruption to cash flows, and increased collection costs."

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 scorecards for decision making and adoption of external ratings for assessment of borrower-ratings,
- Credit administration processes, credit recovery strategies and processes that ensure minimal losses to the company while ensuring borrower rights are honored.

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 management 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.

The Company has a comprehensive and well-defined product level credit policy encompassing the credit approval process. The company shall at all times have a well-structured product level credit policies and procedures that is duly supported by the senior management and approved by the Board of Directors or by a committee appointed by them.

The product level credit policies sets out the guidelines, principles and approach to appraise credit and contains a framework to identify, assess, measure, monitor and control credit risks in a timely and effective manner.

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

- Establish standards for internal credit scoring framework and credit appraisal.
- Establish standards for effective measurement and monitoring of credit risk.
- Maintain credit risk exposures within established credit limits.

- Establish governance, roles and responsibilities across the credit life cycle
- 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 RBI from time to time.

6.1. Risk Practices

The risk team shall monitor the credit risk exposure of the company through the following components forming part of the credit risk management framework:

- ECL monitoring: The ECL calculation process in the company has been automated thus ensuring accuracy and reducing the probability of potential manual errors. The company also performs a comparative analysis of the ECL provision and the waiver on settlement at quarterly intervals to assess the accuracy and sufficiency of the provisioned amount.

- Monthly portfolio updates: The company monitors its loan portfolio on a monthly basis including monitoring of key credit risk metrics such as delinquency rates, credit quality, provision coverage ratio, credit concentration, level and amount of non-performing accounts, etc. The company uses this MIS to identify early warning signals of potential default by the counterparty thus enabling them to take relevant mitigation actions. Monthly portfolio monitoring also enables them to evaluate the performance of various loan portfolios thus enabling them to make informed decisions regarding portfolio diversification and risk mitigation measures. Any issues identified during such monitoring are assessed till the regional and branch level to identify the root cause.

- Hind Sighting audit: A post disbursement audit is performed on a monthly basis by an external auditor. The audit is performed to ensure compliance with the credit policy of the company. Historical loan disbursement transactions are reviewed to identify any instances of deviation from the established credit policies and procedures and assess the impact of such deviation. It shall involve the review of documentation, procedures followed, approvals obtained, and loan disbursed. Any instances of non-compliance can be evaluated to identify the root cause and areas of improvement and in turn strengthen internal controls to avoid such instances in the future.

6.2. Reporting

The risk team is responsible for carrying out the risk management practices as mentioned above on a monthly basis and for monitoring the credit risk metrics forming part of the KRI repository at the required frequency. The credit risk team shall report to the CRO on a monthly basis on parameters such as:

- Expected Credit Loss
- Gross NPA and Net NPA
- Provision Coverage Ratio
- Credit Concentration
- Total Delinquency
- Quick Mortality
- Bounce Ratio
- LTV trends

7. Operational Risk

Operational risk arises due to the failure of controls or a combined failure of people, systems, and processes. Operational risk incidents can also be triggered due to external events. Since operational risk affects all areas of the Company's operations, any failure in the same can lead to failed business objectives. The activities which the company undertakes, exposes it to various types of operational risks and hence the company is required to establish a robust operational risk management system.

The Operational Risk Management practice of the company shall aim at the following:

- Develop a common understanding of Operational Risks across the company, so as to assess exposure with respect to Operational Risks and take appropriate actions
- Develop a robust and comprehensive Operational Risk Management process to commensurate to the organization's risk profile and risk appetite
- Create a culture and environment for the effective management of operational risk in the organization
- Define and implement risk governance and management structure and as per leading industry practices

- Enable the Senior Management and the Board of Directors to embed discussions on risk in their strategic decision-making, pricing, remuneration, etc.
- Strengthen the internal control environment and implement other risk mitigation measures in a cost-effective manner
- Reduction of operational risk losses
- Embed the results of operational risk management processes into day to day business of the organization

Operational Risk Management governance structure shall include the Board of Directors, Risk Management Committee and Chief Risk Officer. The organizational structure for managing operation risks consists of the following three lines of defence:

- First line of defence consists of functions that own and manage the risk which consists of all the business units and support functions through adherence to the laid down procedures
- Second line of defence consists of functions that oversee risks which consists of the Risk Management
- Third line of defence consists of Internal Audit which provides an independent assurance on the effectiveness of governance, risk management, internal controls.

8. Market Risk

Market Risk is the possibility of loss arising from changes in the value of a financial instrument as a result of changes in market variables such as interest rates, exchange rates and other asset prices.

8.1. Currency Risk

The Company does not have any instrument denominated or traded in foreign currency. Hence, such a risk does not affect the Company.

In case of any potential foreign currency denominated instruments, the company shall undertake complete hedging of the principal component of the instrument. With respect to the interest component, the company shall enter into derivative transactions to swap its floating rate obligations for fixed rate obligations. The derivative contracts shall be valued at the counterparty provided MTM on a monthly basis. The company shall not undertake any speculative derivative transactions i.e., all derivative contracts shall be entirely backed by an underlying foreign currency instrument.

8.2. Interest Rate Risk

Interest rate risk is the risk that changes in market interest rates might adversely affect the Company's financial condition. The company shall invest its surplus funds as per its investment policy wherein the objective is to park the surplus funds and maintain sufficient liquidity instead of earning returns. The Company invests its funds in Mutual Funds, Government securities, Treasury bills and its subsidiaries ("IndoStar Housing Finance Private Limited" and "IndoStar Asset Advisory Private Limited").

Investments in Mutual Funds give rise to market risk. The Company utilizes the Value-at-Risk method to determine the potential losses for the mutual fund exposures based on the historical returns of the instrument. The company performs traditional gap analysis and prepares the interest rate sensitivity statement on a quarterly basis to measure the interest rate risk. The prudential limits on individual Gaps have been mentioned in the ALM policy of the Bank and have been approved by the RMC. The company is exploring the possibility of computing Earnings at Risk and setting limits on Net Interest Income to measure the interest rate sensitivity.

9. Liquidity Risk

Liquidity risk that the risk that may arises risk of incurring losses resulting from the inability to meet payment obligations (expected/unexpected) in a timely manner when they become due. The Company uses various tools and metrics to manage its liquidity risk exposure.

The company has a detailed ALM policy and contingency funding planning policy to be able to address any adverse situation on Liquidity position of the company.

9.1. Risk Practices

The ALCO support group shall be responsible for carrying out the following liquidity risk monitoring practices. The liquidity risk metrics shall be calculated manually at the stipulated frequency using excel based models.

- Monitoring of daily liquidity and the surplus / shortage of funds and foresee liquidity and cashflow requirements
- Measuring liquidity risk using the stock approach i.e., monitoring the critical ratios in this regard mentioned in the ALM policy
- Maturity profiling, monitoring of ALM cashflows, and Liquidity Coverage Ratio
- Preparation of Structural Liquidity Statements at the required intervals to measure the difference between Assets and liabilities in each time bucket based on residual maturity of the various line items
- Liquidity, borrowings, and investment research in compliance with the investment and ALM policies and final approval by Head – Treasury and CFO
- Monitoring of funding concentration risk and funding concentration limits based on both lender / counterparty and instrument
- Monitoring compliance with the various limits such as LCR thresholds, ALM limits, stock ratios, funding concentration limits mentioned in the ALM policy
- Liquidity stress testing on a quarterly basis to assess the ability of the company to withstand unexpected liquidity drain without taking recourse to any outside liquidity support
- Monthly analysis and reporting of the contingency funding plan including the escalation matrix and KRIs

Additionally, the treasury team shall monitor the market conditions for possible impact on the cost of funding and liquidity of financial assets.

Enterprise Risk Management Framework

9.2. Reporting

The ALCO support group comprises of members from the Treasury, Finance and Risk team who shall report to the Head-Treasury, CFO and CRO respectively.

The ALCO support group shall submit the liquidity reports on LCR, Structural Liquidity Statement and contingency funding plan to the ALCO on a quarterly basis. It shall also submit the stock ratios report to the ALCO on a quarterly basis.

The ALCO and RMC will closely monitor any mismatch positions and the macro-environment to consider all indicators of risks, to plan and advise suitable action. The Head-Treasury, 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.

The ALCO shall meet on a quarterly basis to discuss the liquidity risk metrics. In case of any breach / deviation from the ALM policy / investment policy / contingency funding plan policy, the impact and mitigation action for such a breach is discussed and the progress is reported in subsequent ALCO meeting.

10. Fraud Risk

Fraud carried out by employees including embezzlement of funds as well as by customers expose the Company to financial losses. The Company has a fraud management unit which investigates frauds and carries out random checks as required.

The company has adopted a fraud risk management policy that covers aspects such as norms for classification of frauds, mechanism of internal reporting of frauds, requirements of reporting to RBI, requirements for review and reporting of frauds to Board and to the Audit Committee, guidelines for frauds reporting to the police, etc.

The Company has documented a Risk Control Unit SOP that outlines the measures to identify, assess and mitigate fraud risks. It includes the procedure for monitoring transactions, conducting due diligence on customers and employees and implementing internal controls. It shall detail the reporting mechanisms for suspected fraud activities.

10.1. Risk Practices

The fraud monitoring team is responsible for fraud risk management which includes risk identification, assessment and mitigation. The team conducts fraud monitoring for different types of frauds viz. pre-disbursement, post disbursement and collateral fraud. The following fraud risk control measures are followed:

- Segregation of duties at various level
- Implementation of maker – checker concept
- Strengthening of internal controls across the Organization
- Implementation of an effective internal audit mechanism
- Implementation of Know your customer policy and guidelines
- Installation of an effective complaint resolution mechanism
- Awareness of fraud risk is created through periodic assessment, training, and frequent communication
- All new credit proposals received should be properly scrutinized, especially in relation to creditworthiness report, purpose for which credit facilities are required and to ensure that the applicant is not a defaulter with any other branch / bank/ financial institution in any other associated / sister concerns etc.
- Strict adherence to the delegation of authorities
- Strict monitoring or supervision of borrowers' accounts, especially big borrowers accounts or accounts causing concern

- Fraud algorithms are run in back end to throw triggers for credit team to check and ensure no fraud application is passed
- Screening and sampling is performed to identify the frauds at exposure level

The company has also adopted the use of an API integrated Hunter check system wherein all the loan applications are verified in the Loan Origination System before approval.

10.2. Reporting

The fraud risk monitoring team reports to the Head-RCU who in turn reports to the CRO. Fraud cases shall be reported to the management at regular intervals and quarterly to the Board and RMC. The company shall also ensure fraud risk regulatory reporting to the RBI at the stipulated intervals.

In addition, internal frauds, i.e., pertaining to employees shall also be reported to the Disciplinary Action Committee. This Committee shall meet on a monthly basis and the Head-RCU shall present the findings to the Committee. The Committee shall review such findings thoroughly and take necessary disciplinary action against the employee such as providing a warning to the employee or termination of employment to avoid such occurrences in the future.

The company shall at all times ensure compliance with the requirements laid down in the RBI Directions pertaining to monitoring of fraud risks[1].

[1] Master Direction - Monitoring of Frauds in NBFCs (Reserve Bank) Directions, 2016

11. Cybersecurity Risk

In accordance with regulatory guidelines, the Company has formulated an Information Security policy. The Policy provides an Information Security framework with basic tenets inter-alia identification and classification of information assets, physical security, network security, wireless security, Incident management, data backup disaster recovery, set up aspects, based on the aforementioned requirements, the Company has adopted the Information Security Standards & Procedures.

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 the company shall apply to its information resources and assets to mitigate various cyber security risks. The company shall implement security controls at all levels to protect the confidentiality, integrity, and availability of information during processing, handling, transmission and storage.

The company has adopted a Comprehensive IT Policy encompassing acceptability of various usages, asset management, applications management, infrastructure management and IT security.

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. The company shall monitor and manage the outsourcing contracts as per the guidelines prescribed by RBI[2] at all times.

11.1. Risk Practices

The following is an overview of the areas of information security risk management conducted by the information security team:

1. Security Operations Center
    - The company has outsourced the 24*7 SOC operations to a third party vendor that monitors the internal traffic and firewall.
    - The third party vendor evaluates and reviews the vulnerabilities, unauthorized access, hacking attempts, etc. and reports the same to the information security team.

[2] Master Direction on Outsourcing of Information Technology Services

- It also prepares bulletins on aspects such as patch and version update and reports the same to the information security team on a daily basis.
- The modifications required as per the SOC report are to be implemented by the IT team of the company. The IS team oversees the implementation of such tickets and changes to ensure that all necessary updates are made in a timely manner.

2. Dark web monitoring
   - The company conducts dark web monitoring for external firewall and vulnerabilities. It aims to identify and mitigate risks associated with cybercrime, such as data breaches and identity theft. The company monitors the mention of sensitive information and compromised credentials on such dark web platforms.
   - Apart from getting quarterly reports from the Computer Emergency Response Team of the Government of India, the company internally monitors instances of such credential compromise and takes immediate necessary action.

3. Training and Awareness
   - The company shares daily e-mails and flyers on different topics with all its employees across all the branches to create cybersecurity awareness.
   - Physical and electronic posters on information security and cybersecurity are created and displayed in every branch of the company.
   - Mandatory onboarding as well as annual trainings on cybersecurity awareness are conducted.
   - Cybercrime simulation sessions are held for the top management of the company.
   - Phishing email simulation sessions are held on a regular basis

4. IT Audit
   - Annual VAPT audit is conducted for all applications and IT infrastructure by a third party. The reports are submitted to and reviewed by the Board and RMC.
   - VAPT analysis of new applications is also conducted before it is implemented in the company.

5. Business Continuity Planning and Disaster Recovery
   - 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 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.
- Annual disaster recovery mock drills are conducted by the IT team and reports are submitted to the cybersecurity team for review.
- Business Continuity Planning training modules have been formed and annual mock drills shall be conducted. It shall include the Business Impact Analysis and the Risk Assessment.
- The company has adopted BCP and DR policies that shall be reviewed (and revised as may be appropriate and necessary) by the Chief Risk Officer and RMC from time to time.

6. Other practices
   - Data storage and access: Database server gets updated online. Only authorized personnel will have access to the database. 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.
   - Applications (software): Only authorized and licensed software will be loaded into the system – central and at various user points. The licensing position will be reviewed periodically to guard against violations of IT Copyrights / Laws.
   - 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 on the central server and at all user points and updated regularly.

11.2. Reporting

The information security team shall report to the Chief Information Security Officer (CISO) who shall in turn report to the CRO, RMC and the Board.

The company has formulated the IT Strategy Committee, IT Steering Committee and Information Security Management Committee for overseeing, managing, and forming mitigation actions for

information security and cybersecurity related risks. Each committee meets on a quarterly basis and is responsible for performing the functions prescribed by RBI[3].

The information security team prepares monthly dashboards on the summary / progress on the above risk practices that is in turn reported to the Information Security Management Committee.

Additionally, the IT team is required to submit reports on a monthly basis to the information security team for ensuring that all requisite information security checks are in place and there are no data leakage and cyber frauds.

[3] Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices

12. Other Risks

12.1. Outsourcing Risk

Outsourcing involves entering into an agreement with another party (including a related body corporate) to perform, on a continuing basis, a business activity which currently is, or could be, undertaken by the Company.

Non-core functions 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.

Outsourcing arrangements present key challenges, which if not addressed adequately, introduce significant risks for the financial institution. These include:

- Managing and monitoring the outsourcing arrangement
- Selecting a qualified vendor and defining the scope of the outsourcing arrangement
- Ensuring effective controls and independent validation
- Reviewing the effectiveness of policies and procedures

The Outsourcing Committee shall include key management persons comprising of below :

(i) Head Compliance
(ii) Chief Credit Officer
(iii) Head Operations
(iv) Chief Technology Officer
(v) Chief Product Officer

The Outsourcing Committee shall be responsible for functions such as:

- approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing and the policies that apply to such arrangements
- undertaking regular review of outsourcing strategies and arrangements for their continued relevance, and safety and soundness
- deciding on business activities of a material nature to be outsourced, and approving such arrangements

- approval for outsourcing based on risks and materiality

The Company has incorporated the risks associated with outsourcing activities and the relationship with the service provider in the Outsourcing Policy and the IT Outsourcing Policy.

The respective Department Head shall ensure the following practices while outsourcing activities to a third party vendor:

- Ensuring that only eligible services are outsourced.
- For approving all outsourcing arrangements related to specific activities entered into by the ICFL.
- Annual review of the outsourced activity will be done by respective functions/departments and put up to the Outsourcing Committee with their comments about the compliance as agreed in the terms of contract and benefit achieved.
- To ensure that all the functional departments have conducted necessary due diligence before entering into any outsourcing arrangement with any vendor.
- To appraise the Risk Management Committee and the Board of all the material contracts entered by the ICFL.
- To ensure that parameters for defining materiality of outsourcing arrangements is correctly defined and updated as per requirements
- To ensure that Vendors are correctly classified as material / non-material vendors.
- To ensure that the Outsourced Vendors perform their duties as stated in the Policy (E.g.:maintaining security and confidentiality of customer information, DSAs comply with Code of Conduct etc)
- In case, there is outsourcing within the group, necessary compliances are followed.
- To review the risks in respect of Material contracts
- To review on an annual basis the performance of vendors/ service providers to whom activities have been outsourced and report the findings for submitting to the Risk Management Committee and the Board.
- To place the summary of outsourcing activities and review of exceptions (if any) to the Board of Directors on an annual basis.
- To check if the criteria for selection of vendor/ service providers is in line with the outsourcing policy or same need any modification.
- To check if the delegation of authority is laid down appropriately depending on risks and materiality as per the outsourcing policy and same need to be reviewed periodically.

- To arrange for the internal audit of material outsources activities on a regular basis and the report of the same shall be placed before the Audit Committee.
- To ensure that no activity is outsourced to an off-shore location
- To ensure that the Grievance Redressal is handled as per Grievance Redressal Mechanism of the Company.

- Key risks such as reputation risk, compliance risk, operational risk, contractual risk, exit strategy risk, etc. shall be considered while outsourcing the contract.
- The expectations of the company should be clearly and fully documented in a formal contract. The Company should negotiate a written contract that is operationally flexible and that clearly articulates the expectations and responsibilities of both the company and the outsourcing vendor.
- The contract for the relationship must articulate the expectations from the vendor, including performance measures and incentives/payouts and the support to be provided by the Company.
- The requirements for the Service Provider should be properly documented and should guide the selection process.
- The selection should be based on the due diligence carried out by the Company on the Service Provider to ensure technical capabilities, managerial skills, financial viability, familiarity with the financial services industry, and a demonstrated capacity to keep pace with innovation in the marketplace.
- Due diligence and reference checks of the agencies will be ensured.
- Review at least once a year all the activities which are outsourced.
- Periodic review and monitoring of activities and control processes of the Service Provider.
- At least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations.
- Consider all relevant laws, regulations, rules, guidelines and conditions of approval, licensing or registration, when performing its due diligence in relation to outsourcing of services.
- A central record of all material outsourcing contracts shall be maintained by the respective responsible Department.
- Maintain a robust grievance redress mechanism, which in no way should be compromised on account of outsourcing.
- Ensure that there are definite contingency plans viable in the event of non-performance by the service provider.

- Ensure that the Outsourced IT service providers periodically tests the Business Continuity and Recovery Plan and may also consider occasional joint testing and recovery exercises with its service provider. It shall evaluate the possibly of bringing the outsourced activity back in-house in an emergency situation.
- Seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.

The company shall monitor and manage the outsourcing contracts as per the guidelines prescribed by RBI[4] [5] at all times.

[4] Master Direction on Outsourcing of Information Technology Services

[5] Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023 (Annex XIII: Instructions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs)

12.2. Compliance Risk

The Company is an NBFC coming under the regulatory purview of the Reserve Bank of India, and the Securities Exchange Board of India. In addition, the Company is also required to comply with various laws applicable in the conduct of the activities of the business.

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 deal with the challenges posed by the changes. The Company will respond effectively and competitively to regulatory changes 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.

The Compliance Team has been entrusted with the responsibility of implementing the Compliance Policy and accordingly it has put in place internal processes to implement the requirements laid down in the Policy. These include dissemination of regulatory guidelines, handling internal queries on regulatory guidelines, acting as the nodal point for regulatory matters (regulatory correspondences, inspections etc.), compliance monitoring process, Board of Directors/Audit Committee reporting, Monthly compliance reports etc.

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 Department of the Company will provide the assurance through the audit of the compliance levels. The company shall at all times ensure compliance with the RBI directives for monitoring of its compliance framework[6] and for filing of supervisory returns[7].

Additionally, the company has employed a compliance monitoring tool for internal monitoring of compliance with regulatory requirements and instructions[8]. The tool enables the company to identify, assess, monitor, and manage compliance requirements. Automated reminders are sent to the relevant stakeholders at regular intervals for the upcoming regulatory requirements and the stakeholder shall be required to upload the proof of such regulatory compliance. MIS reports are generated at quarterly intervals showing a summary of the compliance requirements delayed / breached.

[6] Compliance Function and Role of Chief Compliance Officer (CCO) - NBFCs
[7] Master Direction – Reserve Bank of India (Filing of Supervisory Returns) Directions - 2024
[8] Streamlining of Internal Compliance monitoring function – leveraging use of technology

The Compliance team shall report to the Chief Compliance Officer of the company and is responsible for monitoring the compliance breaches and reporting the quarterly MIS statements to the RMC and the Board.

12.3. Reputational Risk

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) and may be committed either consciously or otherwise. It is the current and prospective impact on earnings and capital arising from the negative opinion of various stakeholders of the company. Reputation risk can affect the company's ability to establish new relationships and services or continue servicing existing relationships. Reputation risk could result in loss of revenues and diminished shareholder value. The company, therefore, considers protecting its reputation of paramount importance.

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, regulatory or compliance breaches, evasion of taxes, charging exorbitant interest rates, dishonoring commitments, etc.

Risks to the Company’s reputation will be addressed by:

- Instituting a strong risk management system including fraud prevention and creating a culture of risk awareness across the organization.
- A commitment to transparency, morality and accuracy in operations including the correctness of financial statements for public use.
- Maintaining a robust and effective communication channel across the organization including all stakeholders such as Directors, Shareholders, Regulators, Lenders, Customers, Employees, Vendors etc.
- Encouraging and rewarding ethical behavior amongst employees. Ensuring immediate but fair action against employees indulging in unethical action or behavior.
- Ensuring prompt compliance with regulatory directives and other laws both in letter and spirit.
- Institutionalizing customer service excellence supplemented with an efficient complaint redressal mechanism.
- Maintaining effective liaison with media and issuing prompt clarifications or rebuttals to negative reports.

The responsibility for protecting the reputation of the Company and taking steps to enhance the Company's standing will lie across all functionaries in the organization which will be regularly overseen by the Chief Risk Officer and reviewed by the senior management.

13. Risk appetite statement

13.1. Overview

The purpose of a risk appetite is to specify the types and amounts of risk the company is willing to accept and make informed decisions on the allocation of resources to managing risk exposures.

The company's risk appetite is integral to its overall risk management approach which comprises amongst others; measures for identifying and assessing risk, implementing and monitoring the adequacy of control measures, managing incidents and breaches, reporting the status of risk, control and remedial actions to the company's governance committees.

This company has documented and adopted a set of Key Risk Indicators (KRIs) to proactively monitor potential risks and threats to its operations. These indicators serve as early warning signals, allowing timely identification and mitigation of risks.

Basis the individual factors contributing to the risk factors, thresholds for each KRI are defined based on past historical data, comparison to industry peers and the company's internal growth and business plans. Each KRI is scored basis a 3-point scale approach divided into High, Moderate and Low with score of 3,2 and 1 respectively. Further, the company has documented the monitoring frequency for each KRI and mitigation actions to be undertaken in case of breach of any threshold.

The Company has considered the below risks and established KRIs for ongoing monitoring and reporting for the same:

- Credit risk
- Market risk
- Operational risk
- Liquidity risk
- Interest rate risk
- Reputational risk
- Compliance risk
- Fraud risk
- Cybersecurity risk
- Outsourcing risk
- People risk
- Business and Strategic risk

The Company has designed a risk appetite statement by identifying the key metrics to be monitored for each risk category. The risk appetite statement considers the most significant risks to which the Company is exposed and provides an outline of the approach to managing these risks. All strategic plans and business plans for functional areas are consistent with this statement.

13.2. Monitoring Guidelines

The KRIs shall be continuously monitored at the frequency mentioned in the master repository of KRIs. These values shall be monitored by the heads of the respective risk teams and the results shall then be consolidated and reported to the CRO and to the senior management at a frequency determined by the Company as appropriate.

The risk appetite statement shall be continuously monitored by the Risk Team. The metrics and their performance shall be reported to the RMC at least on a quarterly basis and may be reported to the senior management at a frequency determined by the Company as appropriate.

The KRIs and Risk Appetite Statement shall undergo a comprehensive review at the end of each financial year whereby the relevance of the metrics and thresholds would be reassessed, and any new metrics identified to be important shall be included. A change in the business environment and/or internal policies may necessitate a review of the KRIs / risk appetite statement, the same shall be undertaken on an ad hoc basis as determined by the Chief Risk Officer in consultation with the RMC and the CEO.

13.3. Risk heatmap and prioritization

The prioritization of risks is a critical aspect of effective risk management and the use of risk heatmap can act as a powerful aid in the process. A risk heatmap visually represents risks based on their likelihood and impact, creating a clear and concise overview of the risk landscape.

In order to monitor the materiality of each risk, the KRIs / metrics are evaluated on the RAG scale to determine the mitigation plan to be initiated and whether the risk levels are within the appetite established by the Company.

The probability or likelihood of occurrence is evaluated by assigning a score to each KRI as follows:

RAG scale	Score
High / Red	3
Moderate / Amber	2
Low / Green	1

A weightage is assigned to each KRI under each risk category and a weighted average score gives the probability score for each risk area. The probability is basis 5-point scale-based system categorized as Very High, High, Medium, Low & Very Low impact as below:

Weighted average score	Likely probability	Score
>2.60 to <= 3.00	Very High	5
>2.20 to <=2.60	High	4
>1.80 to <=2.20	Medium	3
>1.40 to <=1.80	Low	2
>1.00 to <=1.40	Very Low	1

The potential impact of each risk is defined based on the consequent adverse impact on the company in case that risk materializes. The Company has categorized each risk impact basis a 5-point scale into Very High, High, Medium, Low & Very Low impact. The impact has been defined on the basis of past experience, assessment of similar risk on similar nature of business operations.

A product of the probability score and impact score indicates the materiality and significance of each risk for the Company. The same is to be presented by way of a heatmap to understand the relative significance of each risk.

14. ICAAP Policy and document

The Policy on Internal Capital Adequacy Assessment Process reflects an integrated approach to risk management and capital management, involving an assessment of the level of, and appetite for, risk and then ensuring that the level and quality of capital are appropriate to that risk profile. The Company has undertaken a thorough ICAAP assessment including identification and review of material risks, assessment of forward-looking business model and operationalization strategy to assess the impact of material risks on the level and quality of capital.

The policy lays down the material risks, capital quality and level, risk quantification results along with risk management processes and governance followed by the Company in line with the RBI guidelines.

The Company has identified the following material risks and incorporated them in the Pillar II risk assessment program:

- Credit risk
- Market risk
- Operational risk
- Liquidity risk
- Credit concentration risk
- Interest rate risk in banking book
- Strategic risk
- Securitization risk
- Outsourcing risk
- Model risk
- Technology risk
- Legal risk
- Reputational risk

15. Risk reporting

Enterprise Risk Management (ERM) is incomplete without a structured process for reporting risk-related information to all stakeholders, which encompasses reporting to both external and internal stakeholders.

15.1. Risk Reporting to External Stakeholders

External stakeholders typically include regulatory and legislative bodies. As a Systemically Important Financial Institution, IndoStar is required to submit various reports on risk-related information, such as from credit risk, liquidity risk and fraud risk perspective. These reports provide a comprehensive overview of the company's risk profile. The Compliance Department facilitates interactions with regulators and advises internal stakeholders on relevant and current reporting requirements.

15.2. Risk Reporting to Internal Stakeholders

Internal stakeholders encompass various levels within the organization, including the Board of Directors, Board Committees, Senior Management Team, Functional Management Teams, and Operational Stakeholders across all Business Units and Support Units.

Various risk dashboards shall be reported to the internal stakeholders including:

- Reporting of the KRIs to the senior management and functional teams at the mentioned frequency.
- Reports to measure the risk metrics consistently across all functional units and serve as the basis for Management Information System (MIS) reports on the company's risks.
- Various risk reports to be submitted to Committees such as ALCO, Disciplinary Action Committee, Information Security Management Committee, etc. as mentioned in the previous sections of this policy

15.3. Periodic Reporting to the RMC

The CRO submits a detailed summary of the company's overall risk status based on the ERM Framework to the RMC. This status report, presented in the form of a dashboard, includes relevant details to facilitate effective oversight of risk management activities as well as progress on the key risk actionable agreed to in the previous RMC meeting.

Enterprise Risk Management Framework

16. Policy Administration

16.1. Applicability of policy

- This policy governs the ERM framework for the Company.
- This policy will become applicable from the date it is approved by the Board of Directors of the Company.

16.2. Frequency of revision

- The ERM policy shall undergo a review process at least once a year. Every such review will require an approval from the Board of Directors.
- Reviews and modifications during the year may be permitted if there is a specific need for the same due to business, regulatory or other reasons.

16.3. Policy approval process

- This document shall be initially recommended by the Risk Management Committee and approved by the Board of Directors.
- Any subsequent changes will require approval from Risk Management Committee followed by approval from Board of Directors.