RISK MANAGEMENT FRAMEWORK

Standard Capital Markets Limited

Table of Contents

DOCUMENT IDENTIFICATION INFORMATION

Document Name	Risk Management Framework
Index	Operational Risk Management
No. of Pages	33
Approving Authority	Board of Directors
Review Frequency	At least once a year or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

This policy is issued by Standard Capital Markets Limited (hereinafter referred to as "SCML" or "Company").

1. Introduction

1.1. The RBI has mandated the compliance of the "Risk Management Framework" under clause 4.4 of the Guidance Note on Operational Risk Management.

1.2. This policy shall list all the risks that a business unit may encounter during the operations, risk appetite and tolerance defining the risk capacity of the company, and the measures to mitigate the risk for the smooth functioning of the Company.

1.3. The Risk Management Framework is the overall approach, including policies, processes, controls, and systems, through which risk appetite is established, communicated as well as monitored.

2. Objective of the Policy

2.1. The objective of this policy is to keep the Board of Directors and senior management updated on the risks that the business is about to face so as to prevent them from causing

any serious financial, operational, or reputational damage to the company.

2.2. The framework is significant in ensuring growth and managing risk events by introducing an effective risk management system that may address such issues, to achieve the set objectives and goals of the Company.

2.3. This document shall articulate the risk management principles, define risk, and establish a common risk language across the Company. This policy shall be an umbrella policy covering all significant risks that may affect the Company's operational framework.

3. Definition and Interpretations

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

3.2. "Regulatory Entity" shall mean SCML.

3.3. "Risk" is not only an uncertainty about the future or the probability of suffering a loss. It also encompasses the danger that the actual future outcome of an event will deviate from the expected or planned outcome negatively.

3.4. "Risk appetite" is the aggregate level and types of risk an RE is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.

3.5. "Risk Owner" is defined as the person responsible for managing a particular risk.

3.6. "Risk tolerance" is the variation around the prescribed risk appetite that the RE is willing to tolerate.

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

4. Risk Management Principles

4.1. The Company have adopted certain fundamental principles of risk management in order to mitigate risk as follows:

4.1.1. The Company treats the risk management principle as an integral part of the business and, therefore shall not operate separately from the business activities of the company.

4.1.2. The Company always ensures that its risk management principles must contribute in achieving strategic objectives as well as the performance of the company.

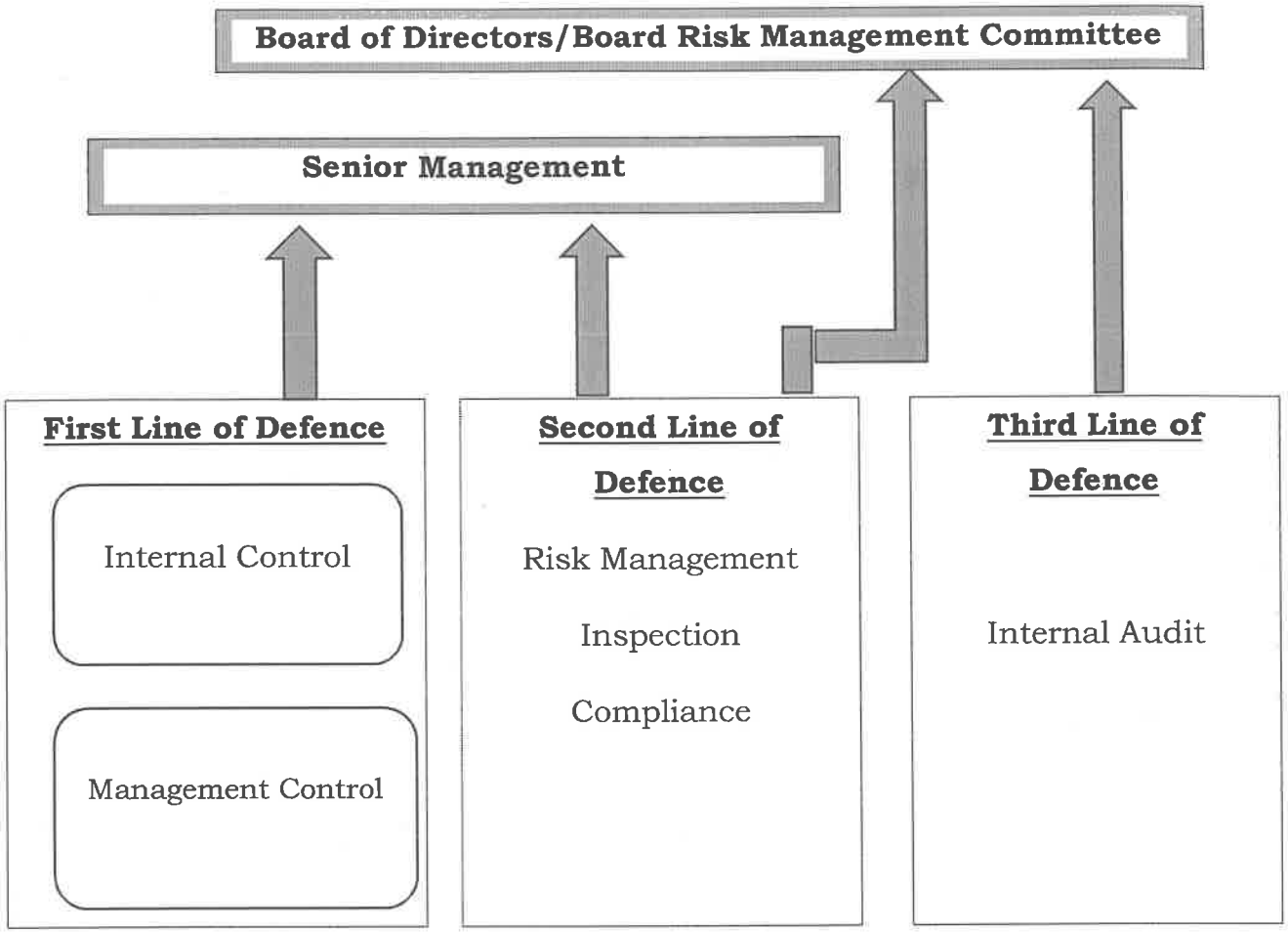
4.1.3. Risk Management framework ensures to aid the decision makers make informed choices, prioritizing actions, and adapting better-suited alternative courses of action.

4.1.4. The risk management at the company is managed based on available sources of information such as historical data, experience, stakeholder feedback, observation, forecasts, and expert judgment.

4.1.5. The Company shall install the required system of risk management to identify risks and implement the controls to mitigate them.

5. Governance Framework

The Company's Operational Risk Management functions in a manner as illustrated in the figure below. This framework outlines the key managerial essentials for effective risk management and the hierarchy followed by the company to mitigate the risk and make an informed decision.



(Governance Structure of Risk Management Framework)

5.1. Risk Owners (Management Head/Department Head):

5.1.1. These are departments/individuals directly responsible for managing specific risks within the Company. They shall be responsible for identifying and assessing the risks in their areas of responsibility and mitigating them accordingly.

5.1.2. The Risk Owners (including Business and department heads) are the part of the **first line of defence** who identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies

and procedures and ensuring that activities are consistent with goals and objectives.

5.1.3. The **Second Line of Defence** shall be the Risk Management Department that shall oversee internal controls and ensure the implementation of the risk management framework. This line is responsible for reviewing established policies, procedures, and regulatory requirements, ensuring compliance with these practices, and monitoring their proper execution.

5.1.4. The Internal Audit shall be the **Third line of Defence** that offers independent checker on Company's operations and lends additional assurance to risk management of the Company.

5.2. Risk Management Committee:

5.2.1. The Company shall establish a risk management committee in consonance with the guidelines.

5.2.2. To assist the board in setting risk strategy policies and discharging its duties relating to corporate accountability and associated risks in terms of management assurance and reporting.

5.2.3. Ensure that the policies and strategies are effectively managed.

5.2.4. To identify the various type of risks involved in the business.

5.2.5. The Chairman of the RMC shall report to the Board regularly and shall meet once a quarter. Further, the findings shall be presented to the Board in the subsequent board meeting.

5.3. Board of Directors:

5.3.1. The Board of the Company has the responsibility for the company's risk management framework.

5.3.2. Defines Risk Appetite Statement and ensures that the risk management process and policies align with the company's strategic goals.

5.3.3. Review and monitor the company's risk profile regularly.

5.3.4. Ensures that a proper risk culture is maintained within the Company, and a well-established governance structure is in place.

5.3.5. The Board may delegate the overall responsibility of the Board to the Head Risk Management to oversee and implement the policy. The delegated personnel shall inform the Senior Management and the Board of all the risks and shall provide periodical reports through "Risk Appetite Breach Report".

5.3.6. Ensure that the Risk Report is part of an Annual Report of the company.

5.3.7. Approve the Business Continuity Plans

5.3.8. Require independent internal audit by well-trained Auditors who are independent of the risk management functions.

5.4. Internal Audit:

5.4.1. They shall review the board policies and procedures.

5.4.2. Evaluate risk management measures and test all aspects of risk activities and positions.

5.4.3. Ensure effective control over management positions and actions. The chair of the Audit Committee of the Board shall be a member of the Risk Committee of the Board.

6. Risk Management Procedure

The Company complies with the following procedure to manage and mitigate the risk. This systematic approach is designed to identify potential risks, assess their impact, and implement appropriate measures to minimize their effects on the Company's operations and

objectives. By following these procedures, the Company aims to create a robust risk management framework that safeguards its assets and ensures a stable and secure business environment.

6.1. Identification and Assessment:

6.1.1. The Company shall install a robust framework that would enable them to identify the internal and external risks that affect the business operations.

6.1.2. Members of the management including heads of the front-line operations shall bear the primary responsibility for identifying risks. They shall be responsible for the assessment and control of credit risk.

6.1.3. Whereas the IT/HR/MIS/Accounts/Finance/Legal and Secretarial Department shall identify, assess and control operational, liquidity and market risk.

These Department heads act as the "first line of defence" in the risk governance framework of the Company.

6.1.4. The dedicated Advisor shall be the "Second Line of Defence" and play a key role in identifying, assessing, and managing the overall risks faced by the Company.

6.2. Manage Risks by Developing Strategies and Implementing Policies:

6.2.1. The Company shall manage the risks by developing risk mitigation strategies that align with the Company's risk appetite and business objectives. This can include risk avoidance, reduction, sharing, or acceptance.

6.2.2. Implement Policies: Establishing policies and procedures to guide the organization in managing identified risks, ensuring consistent application across all functions.

6.2.3. The Board shall manage the risks by adopting following strategies to manage the exposure of risk:

1. Risk Avoidance: The Company may choose to avoid risks which have high probability, are beyond its control and can have devastating effect on its functioning.
2. Risk Transfer: The Company may choose to transfer such risks that have low frequency but can be potentially devastating; examples of tools used for risk transfer are insurance and/or Hedging.
3. Risk Acceptance: If the probability of occurrence and the impact of a particular risk are minor and manageable relative to the cost of controlling it, the Company may choose to accept such a risk
4. Risk Control: If the risk is high and the impact of the risk is low to medium and the costs to manage

it in house is also cost effective, Company may try to control such risks.

6.2.4. The Advisor shall support the management team in developing the strategies and tactics to manage risks.

6.2.5. Every management head is responsible to manage and monitor the identified risks that fall into their work area.

6.3. Test Effectiveness:

6.3.1. The Board of the Company shall regularly test the strategies in place to ensure they are functioning as intended.

6.3.2. Also, conduct audits, simulations, or assessments to measure how well risk management practices are working and if the risks are being properly mitigated.

6.3.3. If there are any requirements for the need of some changes to policies and procedures, the department heads of the company shall suggest new risk control measures.

6.3.4. Internal Audit's role in Risk Management is to assess the effectiveness with which the controls are addressed. The internal audit department shall serve as the control under a direct mandate from the Board. The scope of internal audit specifically also extends to activities of the Managing Director and to verify the effectiveness of the risk management framework.

6.4. Revise Policies and Procedures:

6.4.1. As per the test results and changes in the risk environment, policies and procedures shall be updated accordingly.

6.4.2. Furtherance to the Analysis of the Risk Report and Internal Audit Findings, the Board shall revise the policies and procedures accordingly considering the feedback of the management on the present operational framework/policies and procedures concerning risk.

6.5. Monitor and Control Risks: The risks in the Company's operations shall be monitored and controlled through Key Risk Indicators and other metrics by the Board. Effective Risk Management measures shall be inducted to maintain alignment with the Company's Risk Appetite.

7. Types of Risks

The Company shall encounter the following types of risks in its operations:

7.1. Credit Risk

Definition	The Reserve Bank of India has defined the Credit Risk as, the possibility of losses associated with a decline in the credit quality of borrower/counterparties; or default due to inability or unwillingness of a borrower or counterparty to meet commitments in relation to lending, trading, settlement and other financial transactions; and Loss from reduction in portfolio value.
Causes of Credit Risk	The **primary causes** of Credit Risk may include, but are not limited to: 1. Default on loans: When borrowers are unable or unwilling to repay loans, it results in credit losses for the company. 2. Deterioration in Creditworthiness: A borrower's financial health can decline due to factors like economic downturns, poor business performance, or increased debt, leading to a higher likelihood of default. 3. Concentration Risk: Overexposure to a single borrower, industry, or geographic area can increase credit risk. If that particular sector or borrower faces financial difficulty, the company's loan portfolio may suffer disproportionately. 4. Poor Underwriting Standards: Inadequate assessment of borrowers' creditworthiness during the lending process can result in loans being given to high-risk customers, increasing the likelihood of default.

	5. Market and Economic Conditions: External factors such as recession, inflation, interest rate fluctuations, or geopolitical instability can affect borrowers' ability to repay, increasing credit risk. 6. Lack of Proper Monitoring: Failing to continuously monitor and reassess the risk of existing borrowers can result in delayed identification of potential defaults.
Mitigating Measures	To mitigate Credit risks, the Company shall implement the following **mitigating measures**: 1.1.1.1. Robust Credit Assessment and Underwriting procedure: Before approving loans or extending credit, the company should implement a rigorous credit assessment process. This includes analyzing the borrower's financial statements, credit history, debt levels, and repayment capacity. Underwriting standards should be aligned with the company's risk appetite and regulatory requirements. 1.1.1.2. Credit Scoring System: The credit policy shall mandate that the Company shall use only reliable credit scoring models to help quantify the risk associated with each borrower. These systems can be based on both quantitative data (financial ratios, credit history) and qualitative factors (industry trends, management quality). 1.1.1.3. Risk Limits: The Company shall define the clear risk limits for credit exposure based on its risk appetite.

	1.1.1.4. Stress Testing: The Company shall conduct stress tests to evaluate how the loan portfolio would perform under adverse economic scenarios. This helps assess the company's vulnerability to credit losses and enables proactive management of high-risk exposures. 1.1.1.5. Monitoring and Early Warning System: Continuous monitoring of borrowers financial ability/loan repayment schedules are crucial. The Company shall install an early warning system that detect signs of distress, such as delayed payments, declining revenues, or breaches of financial covenants. These systems help address potential problems before they lead to default.
Governance Framework	1. Board of Directors: The Board holds responsibility for overseeing the management of credit risk within the organization. It approves the credit risk management policy, risk appetite, and overall governance structure. The Board ensures that management takes appropriate steps to control credit risk in line with regulatory requirements and the company's strategic goals. 2. Risk Management Committee: 2.1. Is responsible for overseeing the Company's credit risk strategy and ensuring its alignment with the organization's risk appetite. 2.2. Reviews credit risk reports, approves large credit exposures, and ensures compliance

	with the established credit risk policies and frameworks. 2.3. Monitors overall credit portfolio performance, credit risk concentration, and emerging risks. 3. Credit and lending departments (**First Line of Defence**) are responsible for identifying, assessing, and managing credit risk as part of their daily operations. They execute the credit risk strategy by originating loans, conducting credit assessments, and ensuring adherence to the established credit risk policies. 4. Compliance- Credit Risk Management Function (**Second Line of Defence**): 4.1. The Credit Risk Management function plays a central role in structuring and implementing the credit risk management framework/policies/procedures. 4.2. It shall develop the credit risk assessment tool, credit approval process and credit risk monitoring mechanism. 4.3. It shall monitor the credit portfolio of the borrower and identify concentration risks and implement the Early Warning Signals. 4.4. Provide regular credit risk reports to senior management, RMC, and the Board. 5. Internal Audit (**Third Line of Defence**): 5.1. It shall independently review the effectiveness of the credit risk governance framework.

	5.2. It shall conduct periodic audit of the credit risk management function, business units, and overall portfolio health. 5.3. Provides recommendations to strengthen the credit risk management framework and improve governance.
7.2. Liquidity Risk	
Definition	Liquidity risk arises when a company cannot generate or access sufficient cash to cover immediate liabilities or are unable to meet its financial obligations as they become due.
Causes of Liquidity Risk	The **primary causes** of Liquidity Risk may include, but are not limited to: 1. Mismatched Cash Flows: A key cause of liquidity risk is the misalignment between cash inflows (revenues, receivables) and cash outflows (expenses, debt repayments). If a company's cash outflows exceed inflows in the short term, it may struggle to meet its obligations. 2. Over-reliance on Short-term Funding: Companies that depend heavily on short-term borrowings or credit lines to finance operations face higher liquidity risk. Any sudden tightening of credit markets or increased borrowing costs can lead to a liquidity crunch. 3. Delayed Receivables: When customers delay payments or default on receivables, a company may experience cash flow issues. This is especially problematic for companies

	that have significant accounts receivable but limited cash on hand. 4. Unforeseen Operational Disruptions: Events like supply chain disruptions, equipment breakdowns, or labour strikes can halt production or operations, reducing revenue and cash inflows while costs and liabilities continue to accumulate. 5. Economic or Market Shocks: External factors, such as economic recessions, inflation, currency fluctuations, or geopolitical instability, can limit access to financing and reduce cash inflows, increasing liquidity risk. 6. Poor Financial Planning and Forecasting: Inadequate financial planning, including the failure to accurately forecast cash flow needs or set aside liquidity reserves, can cause a company to be unprepared for sudden liquidity demands. 7. Dividend and Debt Obligations: Committing to large dividend payments or having significant debt servicing requirements (principal and interest payments) can strain liquidity, especially when revenue is not sufficient to cover these obligations.
Mitigating Measures	To mitigate Liquidity risks, the Company shall implement the following **mitigating measures**: 1. Proper Compliance of Liquidity Risk Management Framework shall outline the sufficient liquidity and procedures that are

	required to meet the company's obligations as they become due. 2. Holding sufficient cash reserves provides an immediate buffer for meeting short-term liabilities. 3. Implement early warning indicators that signal potential cash shortfalls, allowing the company to take proactive action. 4. Rely on multiple channels of funding such as bank loans, bonds, equity financing, and internal cash generation. This reduces the risk of overdependence on one source of funds. 5. Develop a contingency funding plan outlining steps to be taken in case of a liquidity crisis. This could involve drawing on credit lines, liquidating assets, or issuing short-term debt. 6. Regularly conduct stress tests to simulate liquidity stress scenarios, such as economic downturns, reduced revenues, or tightening credit markets. This helps ensure preparedness for potential liquidity strains. 7. Ensure compliance with regulatory liquidity requirements, such as the policy of Liquidity Risk Management Framework, the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR).
Governance Framework	1. Board of Directors: 1.1. The board is responsible for setting the Company's overall risk appetite, approving the liquidity risk

management policy and ensure that the governance structure are in place.

1.2. Regularly reviews liquidity risk exposure reports.

2. Risk Management Committee:

2.1. The RMC oversees the liquidity risk management function, ensuring it aligns with the company's risk appetite and regulatory requirements.

2.2. Reviews liquidity risk strategies, stress test results, and potential liquidity vulnerabilities.

2.3. Approves liquidity limits, funding plans, and stress testing frameworks.

2.4. Monitors liquidity risk exposures and early warning indicators.

2.5. Ensures adherence to regulatory liquidity standards.

3. Treasury Function (**First Line of Defence**): The treasury function manages the company's liquidity on a day-to-day basis. It is responsible for cash flow management, funding operations, and ensuring the company has sufficient liquid assets to meet short-term obligations.

4. Liquidity Risk Management Function (**Second Line of Defence**):

4.1. Establishes and updates the liquidity risk management policy, aligning it with regulatory guidelines and the company's risk appetite.

	4.2. Conducts regular stress testing and scenario analysis to evaluate the company's liquidity resilience in adverse conditions. 4.3. Provides timely reports on liquidity risk exposure, stress test results, and limit breaches to senior management and the Board. 4.4. Monitors liquidity metrics such as the Liquidity Coverage Ratio (LCR), Net Stable Funding Ratio (NSFR), and other key indicators. 5. Internal Audit **(Third line of defence):** 5.1. It reviews policies, processes, and controls related to liquidity risk and assesses their robustness.
7.3. Operational Risk	
Definition	"Operational risk" means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. It includes legal risk, but excludes strategic and reputational risk and it is inherent in all banking/financial products, activities, processes and systems. For third party risks the company has a separate policy outlining the management framework and mitigation procedure with regard to the same under "Third Party Risk Management

Causes of Operational Risk	The **primary causes** of Operational Risk may include, but are not limited to: 1. Poorly designed or outdated business processes can lead to inefficiencies, errors, or delays, increasing operational risk. This includes gaps in workflows, poor control mechanisms, or a lack of process standardization. 2. Inadequate employee training on the operational framework can lead to increased operational risk or failures. A lack of risk awareness at both the management and employee levels may also raise the likelihood of risk events occurring. 3. Cyberattacks, inadequate IT infrastructure, poor system integration, and Technology disruptions, such as hardware failures, network outages, or software glitches, can halt critical operations, causing significant delays or loss of business. 4. Events such as earthquakes, floods, hurricanes, or fires can disrupt operations, damage assets, and cause significant financial losses. Companies may face business continuity issues if they are not adequately prepared. 5. Failure to comply with policies, applicable laws and regulations can lead to penalties, legal disputes, and reputational damage.

	6. Lack of proper storage of documents can result in the misplacement of significant files/documents.
Mitigating Measures	To mitigate Operational risks, the Company shall implement the following **mitigating measures**: 1. Establish a structured framework with clear segregation of duties to prevent causing such risk. 2. Regular conduct of Risk Control Self-Assessments to identify operational risks within each department or process. 3. Develop and monitor Key Risk Indicators to detect potential risk events early. KRIs act as warning signals that trigger corrective actions when certain thresholds are breached. 4. Conduct scenario analysis to evaluate the impact of extreme but plausible operational risk events. This shall prepare the company for potential worst-case scenarios and inform risk mitigation strategies. 5. Provide adequate Staff Training on Operational Risk Management, Internal Controls and Compliance Requirements to identify and mitigate such operational risks. 6. Foster a Risk Awareness Culture in the Company so that the employees at all levels understand the occurrence of risk and the importance of mitigating the same. 7. Ensure strong IT System and cybersecurity Measures, and well establish/updated automated systems.

	8. The Company shall maintain all the original documents and store them safely.
Governance Framework	1. Board of Directors: The Board has ultimate accountability for operational risk management. It defines the company's risk appetite and oversees the implementation of a robust risk governance framework. 2. Senior Management: It is responsible for implementing the operational risk strategy defined by the Board. They ensure that risk management processes are integrated into day-to-day operations. 3. Risk Management Committee: The committee ensures that operational risks are properly identified, assessed, and managed across all departments. They shall review the Operational risk reports & incident report, approve and monitor Key Risk Indicators, and ensure that the resources are allocated property so as to manage such risks. 4. The First Line of Defence is the individuals/departmental heads of the Company such as Legal/IT/Account etc. 5. The Second Line of Defence consists of functions that oversee risks which, herein consists of the Risk Management and Compliance Department. 6. The third Line of Defence consists of functions that provide independent assurance provided by Internal Audit which provides the independent Assurance on the effectiveness of

	governance, risk management, and internal controls.
	7.4. IT Risk
Definition	1. IT Risk is defined as the business risks associated with the use, ownership, operation, involvement, influence, and adoption of Information Technology (IT) within the Company. This includes risks arising from the deployment and management of IT systems, software, hardware, networks, and information assets that are integral to the Company's business operations and decision-making processes. 2. IT risks can be broadly categorized into several types, including but not limited to: 2.1. Cybersecurity risks, these risks are associated with potential threats or vulnerabilities that could lead to unauthorized access, data breaches, cyber-attacks (such as phishing, malware, ransomware), and exploitation of system weaknesses. They pose significant risks to the confidentiality, integrity, and availability of information. 2.2. data privacy risks, involving the unauthorized access or leakage of sensitive information; 2.3. operational risks, caused by system failures, software bugs, or infrastructure breakdowns that disrupt business processes;

	2.4. vendor risks, related to third-party service providers or outsourced IT functions; and; 2.5. project risks, stemming from IT project delays, budget overruns, or implementation failures.
Causes of IT Risk	The **primary causes** of IT Risk may include, but are not limited to: 1. Risks arising from hacking, phishing, malware, ransomware, and other cyber-attacks that may compromise the integrity, confidentiality, and availability of the Company's data and IT systems. 2. Risks due to failures or breakdowns in critical IT systems, databases, and networks, which could disrupt business continuity and affect operations. 3. Unauthorized access or leakage of sensitive data that could damage the Company's reputation, result in financial losses, and expose the Company to legal liabilities. 4. Risks associated with reliance on external IT service providers and vendors for critical services, which could impact operations in the event of their failure or non-compliance with security standards. 5. Risks of non-compliance with IT-related laws, regulations, and guidelines issued by regulatory bodies, including data protection regulations and cybersecurity guidelines.
Mitigating Measure	To mitigate IT risks, the Company shall implement the following **mitigating measures**:

	1. Security Protocols: Deploy robust cybersecurity measures such as firewalls, encryption, and multi-factor authentication to protect information assets against unauthorized access and cyber threats. 2. Risk Assessments: Conduct regular risk assessments, including vulnerability assessments, to proactively identify potential IT risks and implement appropriate measures to address them. The risk assessment should be brought to the notice of the Senior Management and the Board of the NBFC and should serve as an input for Information Security auditors. 3. Incident Response Plan: Maintain an incident response plan for timely and effective handling of IT incidents, including cyber-attacks and data breaches, to minimize impact and ensure swift recovery of operations. 4. Training and Awareness: Provide regular training programs for employees to enhance awareness of IT risks, best practices for cyber hygiene, and compliance with security protocols. 5. Vendor Management: Implement a vendor risk management process to ensure that third-party service providers adhere to the Company's security standards and regulatory requirements.
Governance Framework	1. Senior Management: Responsible for ensuring that effective IT risk management processes

are in place, promoting a culture of IT risk awareness and cyber hygiene across the Company, and aligning IT risks with the Company's overall risk appetite and business strategy.

2. The **first line of defence** includes the IT operations teams and business units that use technology systems. They are responsible for managing day-to-day IT risks and ensuring that controls are embedded into their processes.

   2.1. Head of IT Function Accountable for the assessment, evaluation, and management of IT controls and IT risks, including the implementation of robust internal controls and ongoing monitoring of the IT environment to ensure resilience against emerging threats.

3. The Risk Management Committee of the Board (RMCB) are the **second line of defence** that in consultation with the ITSC shall periodically review and update the same at least on a yearly basis.

   3.1. Information Technology Strategy Committee (ITSC):

   The ITSC shall ensure that the Company has in place comprehensive processes for the identification, assessment, and management of IT and cybersecurity risks. The ITSC shall

	periodically review the effectiveness of IT risk controls, approve IT risk assessments, and ensure compliance with relevant regulatory requirements. 3. The third line of defence is **Internal Audit**, which provides independent assurance on the effectiveness of IT risk management processes and controls.
7.5. Market Risk	
Definition	Market Risk refers to the potential for financial losses due to unfavourable changes in market conditions. It arises from fluctuations in the prices of assets, interest rates, foreign exchange rates, or commodity prices.
Causes of Market Risk	The **primary causes** of Market Risk may include, but are not limited to: 1. Interest Rate Fluctuations 2. Fluctuations in the Equity Market can lead to significant losses. 3. Regulatory changes, tariffs, or new policies in major economies can trigger market volatility. 4. Downgraded by credit rating agencies. 5. Global financial crises, pandemics, or systemic failures within financial institutions can lead to widespread market disruptions and large-scale risk.
Mitigating Measures	To mitigate Market risks, the Company shall implement the following **mitigating measures**: 1. Spread investments across different asset classes/industries or sectors.

	2. Regularly conduct stress tests to evaluate how portfolios and financial positions would perform under extreme but plausible market conditions. 3. Use an adequate risk management system to track market risks in real time, providing early warnings when risk thresholds are approached or exceeded.
Governance Framework	1. Board of Directors: The Board of the Company shall oversee the framework of strategies to deal with such risks. The board ensures that market risk management aligns with the company's long-term goals and that risks taken are within acceptable limits. Furthermore, the board are to monitor and ensure the risk limits set for the company are adequate aligning with the Company's risk tolerance. 2. Risk Management Committee: 2.1. Comprises Senior Management and oversees the implementation of the risk management policy. 2.2. Monitor the company's market risk exposure and assess whether it is within approved limits. It shall review risk reports and evaluate market risk management performance. 3. Those involved in trading, treasury, and investment activities, are the **first line of defence** in managing market risk. 3.1. They are responsible for identifying, assessing, and managing their own

	market risk exposures in line with the company's risk appetite and policies. 3.2. Execute trading and investment strategies, ensuring adherence to risk limits. 3.3. Monitor real-time market conditions and respond to market movements by adjusting positions, hedging, or taking other risk mitigation actions. 3.4. Ensure proper documentation and reporting of market transactions. 4. Risk Management and Compliance function are the **Second line of defence.** 4.1. Continuously assess market risks across the company by monitoring exposure to interest rates, equities, commodities, and foreign exchange markets. 4.2. Measure market risk using metrics such as Value-at-Risk (VaR), stress testing, and scenario analysis. Regularly report these risks to senior management and the Board. 4.3. Ensure the company adheres to legal and regulatory requirements related to market risk, such as capital adequacy standards or specific market conduct rules. 5. The **third line of defence** for market risk involves Internal Audit which provides independent assurance of such market risk. The objective of this line is to assess compliance with established procedures, provide

	recommendations for improvement, and ensure that the risk management framework aligns with regulatory requirements and industry best practices.

8. Risk Appetite Statement

8.1. In pursuance of the requirement of Principle-4 of the Guidance Note on Operational Risk and Operational Resilience dated April 30, 2024 which mandates that the company shall have a board-approved Risk Appetite and Tolerance Statement for operational risks, SCML has adopted and approved a 'Risk Appetite and Tolerance Statement' document which includes the nature, types, and levels of operational risk the company is willing to assume.

8.2. The Board has considered the interests of the Company's customers and stakeholders as well as regulatory requirements while structuring the framework of such a statement.

9. Approval, Review & Update

9.1. The Board shall approve the operational resilience approach of the Company and, shall also consider the risk appetite statement and tolerance mechanism to prevent the company from facing severe consequences.

9.2. This policy shall be reviewed annually by the Board to ensure it remains updated and effective. The review process will incorporate feedback from stakeholders to continuously enhance the risk management framework.

9.3. The Company shall update the policy when there are any new changes introduced by the guidelines/ directions issued by RBI

or as and when it is found necessary to change the policy due to business needs.