SHOPPERS STOP

RISK MANAGEMENT POLICY AND FRAMEWORK

OF

SHOPPERS STOP LIMITED

Version	1.0
Board Approval	May 21, 2021

Version	2.0
Board Approval	January 20, 2026

Table of Contents

1. Purpose and Scope of the Policy

The purpose of the risk management policy is to provide guidance regarding the management of risk to support the achievement of corporate objectives and comply with applicable regulations. The policy enables a proactive approach in identifying, evaluating, reporting, and managing risks associated with the business. To achieve the key business objectives, the policy establishes a structured and disciplined approach to Risk Management to manage risk related issues.

The specific objectives of the Risk Management Policy are:

- To enable visibility and oversight of the Board on risk management system and material risk exposures of the company.
- To ensure all risks across the organization are identified and evaluated through standardized process and consolidated across the organization to identify the key risks that matter to the organization to enable risk prioritization.
- To ensure mitigation plans for key risk are agreed upon, assigned to risk owners, and reviewed on a periodic basis.
- To ensure that risk management activities are reported to internal & external stakeholders appropriately.
- To ensure that risk governance structure is aligned with organizational structure and risk profile of the company with well-defined and delineated roles, responsibility, and delegation of authority.
- To enable transparency of risk management activities with respect to internal and external stakeholders.
- To enable compliance with appropriate regulations, wherever applicable, through the adoption of leading practices.

1.1. Scope of the Policy

The policy guidelines are devised in context of the organization's growth objectives, its business and strategy plan, global ERM standards and leading ERM practices. The **Scope of the Policy** shall cover:

- Shoppers Stop Limited and its subsidiaries.
- All functions and locations of the Company
- All events, both external and internal, shall have significant impact on the objectives of the organization.
- This framework and policy shall be reviewed on events such as changes in the business environment/ regulations/ standards, organization structure or upon directives of the Board /Audit committee/Risk management committee.

2. Review and updating of the policy

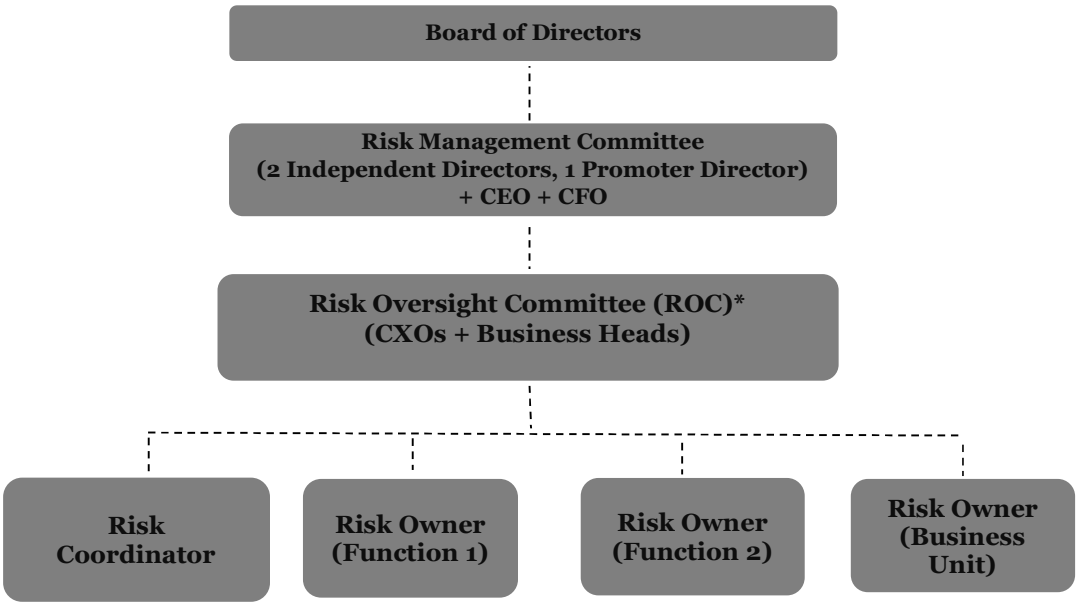
The policy shall be reviewed by the RMC once every two years or upon significant events such as changes in business environment, regulations, or organizational structure.

The ERM policy is integral to SSL's planning and operations, enabling the company to navigate uncertainties and capitalize on opportunities effectively. It supports sustainable growth and value creation for stakeholders.

3. Risk Governance Structure

3.1. Risk Management Organization Structure

A well-defined risk governance structure serves to communicate the approach of risk management throughout the organization by establishing clear allocation of roles and responsibilities. SSL shall set up risk management organization structure which will ensure that risk management activities are undertaken as per the policy.



The Board of Directors of the Company shall constitute the Risk Management Committee consisting of members as may be decided by the Board of Directors.

Committee is authorized to monitor and review the Risk Management plan, and the Board may delegate such other functions, roles, and responsibilities as it may deem fit.

3.2. Roles and Responsibilities

Risk Management Committee (RMC): The composition and quorum of the RMC shall be governed by the applicable regulation. In line with the current regulation (SEBI LODR), the Company has constituted a 3-member committee with 2 independent directors, Promoter and Audit Committee Chair. Their responsibilities include:

- Develop, formalize, and obtain approval for a comprehensive Risk Management Policy.
- Establish and maintain appropriate methodologies, processes, and systems to effectively identify, monitor, and assess risks inherent to the company's business operations.
- Oversee and monitor the implementation of the Risk Management Policy, including periodic evaluation of the adequacy and effectiveness of the company's risk management frameworks and controls.
- Provide the Board of Directors with regular and detailed updates on the nature and outcomes of Risk Management Committee (RMC) deliberations and recommendations, along with subsequent actions undertaken.
- Conduct a biannual review of the risk management processes to maintain their relevance and effectiveness.

- Undertake a formal review of the Risk Management Policy at minimum once every two years to reflect evolving risks and regulatory requirements.

RMC has powers to seek information from any employee, obtain outside legal or other professional advice, and secure attendance of outsiders with relevant expertise, if required.

Risk Oversight Committee (ROC): The ROC shall comprise of CEO, CFO, CHRO, Business CXOs, IA, and Chief Compliance Officer. Managing Director/ CEO to chair the committee. ROC shall work towards establishing and implementation of risk management process effectively in the company. Further, ROC shall nominate additional members for ROC meetings as and when the requirement for more departments' representation arises.

Their responsibilities include:

- Promote the significance of risk management and cultivate a robust risk-aware culture across the organization.
- Oversee the establishment and continuous maintenance of the Risk Management Policy.
- Review and evaluate both existing and proposed strategies for managing key business risks.
- Adopt a comprehensive enterprise-wide perspective towards risk management and address interdepartmental dependencies accordingly.
- Approve the appointment of risk owners, ensuring that appointed individuals hold sufficiently senior positions within the organizational hierarchy to effectively discharge their responsibilities.
- Monitor that risk owners fulfill their duties in identifying, assessing, and regularly reporting relevant risks pertinent to their respective functions or areas.
- Evaluate the ratings of identified enterprise risks and prioritize them for presentation to the Risk Management Committee (RMC).
- Assess and analyze key anticipated risks and associated mitigation measures, recommending additional controls or measures where necessary.
- Verify that effective risk mitigation plans are established, with outcomes regularly evaluated and appropriate actions taken.
- Serve as custodian of the Risk Register, coordinating with risk owners to ensure its timely and accurate periodic updates.

Risk Owner(s): Risk Owners (ROs) shall be the Heads of respective functions or personnel nominated by functional heads and approved by the ROC on time to time basis depending on the organizational structure and business imperatives so as to ensure that all critical and significant enterprise risks are captured while identifying, assessing and managing risks. ROs will be responsible for identification of risks emerging from these decisions, ensuring discussions on these risks and measures for mitigation of these risks in this meeting.

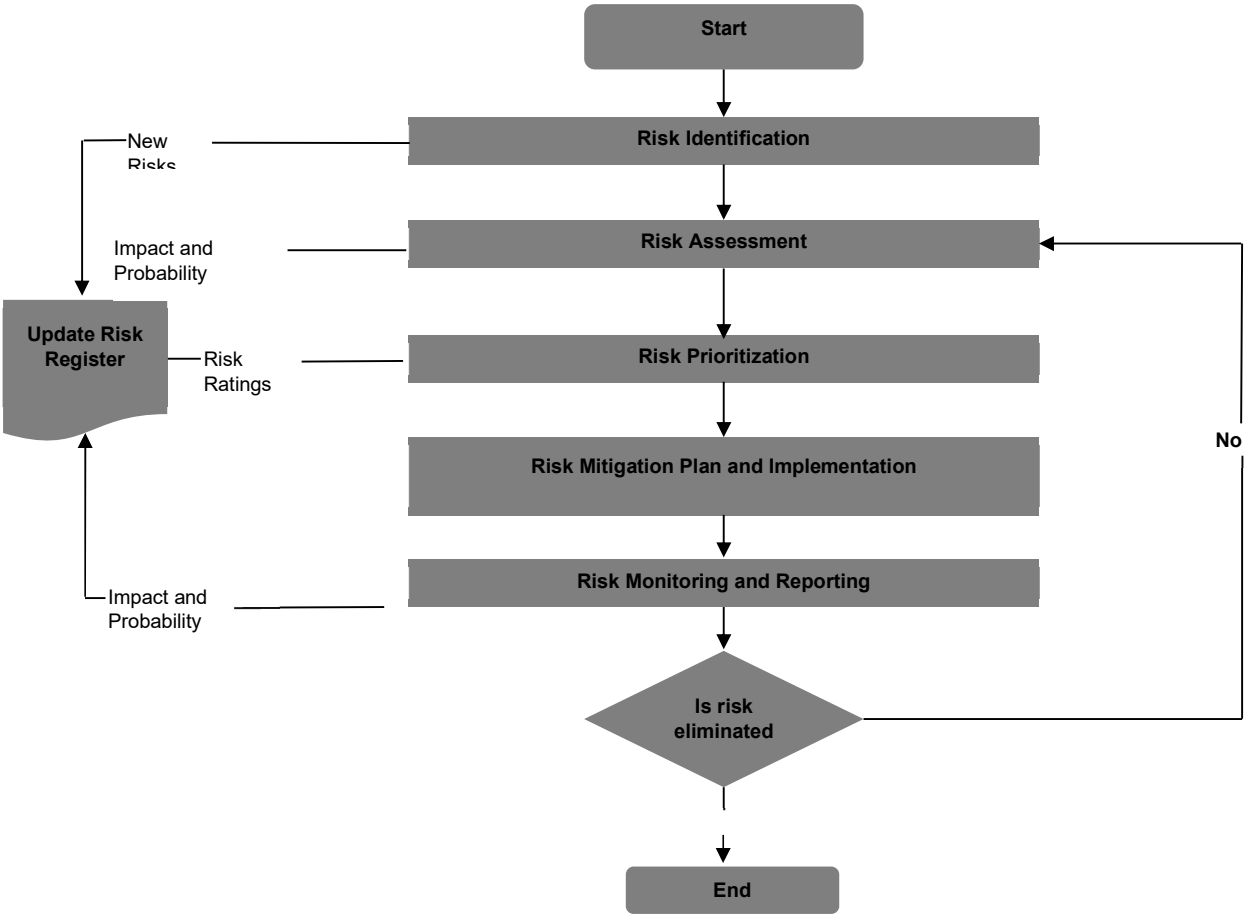
Their responsibilities include:

- Identify risks pertaining to their respective functions or departments.
- Conduct risk assessments in accordance with the established risk assessment framework.
- Align risk mitigation plans with the identified risks.
- Submit risk reports, including assessments and mitigation measures, on a semi-annual basis to the Risk Oversight Committee (ROC) prior to updates presented to the Risk Management Committee (RMC).
- Actively participate in and contribute to periodic ROC meetings.
- Support the implementation of risk mitigation plans approved by, and other directives issued from, the ROC and RMC.

4. Risk Management Process

The management of risk encompasses strategic, operational, and compliance risks that may affect any of the organization's business activities and objectives. This framework establishes the requirements for Departments to develop and implement robust risk management systems aimed at the identification, evaluation, and control of risks. Risk management is conducted through a systematic process involving the identification of risks, assessment of their severity, and evaluation using tools such as the Risk Map and Risk Rating, which consider both the probability of occurrence and potential impact. Management decisions regarding risk control are guided by the four Ts: Treat, Transfer, Tolerate, or Terminate. Periodic reviews of the risk management process are carried out via risk committee meetings at various organizational levels, complemented by Internal Auditing and Continuous Monitoring activities.

The risk management process includes following activities: Risk Identification, Risk Assessment, Risk Prioritization, Risk Treatment and Monitoring & Reporting as shown in the figure below:



4.1. Risk Identification

Continuous identification of risks through workshops, interviews, surveys, and business review meetings. Risks are classified into categories: Macro, Strategic, Operational, Cyber Security & Data Privacy, and Compliance. The assessment process involves evaluating the spectrum of potential consequences alongside the likelihood of their occurrence. Both consequence and likelihood are systematically reviewed to derive an informed estimate of the overall risk level.

4.2. Risk Categorization

For better risk identification, it is important to know various risk categories. Some sample categories are provided below:

Risk Category	Definitions
Strategic	Potential risks affecting high-level goals, aligned with and supporting the entity's mission/ vision.
Operational	Potential risks affecting the effectiveness and efficiency of the entity's operations. They vary based on management's choices about structure and performance.
Compliance Risk	Risk relating to adherence to relevant laws and regulations.
Financial	Potential risks affecting the performance and profitability goals of the company, including safeguarding resources against financial losses.

All emerging risks shall be discussed with the Risk Owners and recorded in the Risk Register.

Refer Annexure 1 for risk register template.

4.3. Risk Assessment

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Risk identified shall be classified into internal, external, controllable, and uncontrollable and assessed for potential severity as per risk rating parameters.

It is necessary that risks be assessed after taking into account the existing controls, to ascertain the current level of risk.

Based on the assessments, each of the Risks shall be plotted on a Risk Assessment table and can be categorized as – Low, Medium and High.

The assessment parameters to rate the impact and likelihood of event occurrence of the risk are mentioned in the table below:

Risk Likelihood

Likelihood Assessment Parameters			
Rating	**Low**	**Medium**	**High**
Occurrence	Events may occur only in exceptional circumstances. Onset of risk event occurs in a matter of several months. No define history of the event	Events could occur at some time or occur in most circumstances. Onset of risk event occurs in a matter of a few months. History of near miss	Event is expected to occur in most circumstances or Very rapid onset of risk event, little or no warning, instantaneous Definite history of occurrence

Risk Impact

SCORE		1	2	3	4	5
RATING		**Low**	**Moderate**	**Major**	**Significant**	**Critical**
STRATEGIC	**Reputational**	Localized Complaints	Repetitive public complaints	Negative local media coverage	Short term negative coverage in national media	Continuous negative coverage in national & International media
	Strategy execution	Minimal risk of failing to execute strategic plans; all key objectives expected to be met without significant obstacles.	Partial inability to execute minor elements of strategic plans; overall objectives remain achievable.	Partial inability to execute one or more non-critical elements of strategic plans, potentially causing minor delays or adjustments in meeting objectives	Potential partial inability to execute a critical element of the strategic plan, likely impacting overall progress toward objectives.	Inability to execute key strategic plans and objectives fully, significantly jeopardizing organizational goals and outcomes.
OPERATIONS	**Business disruption**	Less than 2 working hours	> 2 working hours but < 4 working hours	> 4 working hours but < 8 working hours	>6 hours but < 8 hours	> 8 hours
COMPLIANCE	**Legal/Regulatory**	Insignificant or no impact	Minor compliance failures detected but waived / condoned	Warning show cause legal notice	Penalty upto 50 lakh	- Penalty of more than 50 lakh - Partial /complete prohibition of conducting business - Imprisonment of Key Management Personnel
FINANCIAL	**Revenue**	Up to INR 16 crs	>INR 16 crs and up to INR 33 crs	Over INR 33 crs and up to 66 crs	Over INR 66 crs and up to INR 165 crs	> 165 crs
	EBITDA decline	< INR 0.5 cr	> INR 0.53 crs – INR 2.65 crs	INR 2.65 crs - INR 5 crs	INR 5 crs - INR 10 crs	> INR 10 crs
	Asset erosion	Up to INR 1 cr	Over INR 1 cr and up to INR 5 crs	Over INR 5 crs and up to INR 7 crs	Over INR 7 crs and up to INR 9 crs	> INR 9 crs
EMPLOYEES	**Attritions of employees (SO) per annum**	<10%	Over 10% and upto 15%	Over 15% and upto 20%	Over 20% and upto 25%	> 25%
	Attritions of employees (Stores) per annum	<15%	Over 15% and upto 25%	Over 25% and upto 40%	Over 40% and upto 50%	> 50%

Risk appetite shall be defined for both identified and potential risks and integrated into the formulation of strategies, business plans, execution of business initiatives, performance management, and policy development. The defined risk appetite will be communicated by management, formally endorsed by the Risk Management Committee (RMC), and effectively disseminated throughout the organization. It is imperative that all decision-makers are well-informed of the established risk appetite, enabling them to operate within these parameters while executing their responsibilities to achieve the organization's business objectives.

4.4. Risk Prioritization

Risk prioritization is the process by which the complete set of identified risk events, along with their impact assessments and probabilities of occurrence, are systematically evaluated to establish a ranking from most to least critical. The primary objective of this prioritization is to provide a clear basis for the effective allocation of resources towards the management of risks.

Risk prioritization shall be conducted by Management basis the scoring of the risks.

The impact for a particular risk shall be assessed on the following areas,

- If a particular risk impacts multiple areas, the highest rating will be considered.
- For example, if a particular risk has a 'High' Financial Impact and a 'Low 'Regulatory Compliance Impact, the final impact rating for the risk will be 'High.'

The final risk rating can be obtained from the table based on the values assigned against each of the risks identified.

Parameters	Low	Medium	High
Likelihood	1	5	10
Impact	1	5	10

Measure of Risk Exposure is given below:

For example, if the

Likelihood is High then Impact is High

The final risk rating is as follows: 10*10 =100

Risk Rating Score	Color Coding
1-25	Green
25-75	Amber
>75	Red

Based on the "Severity" and "Appetite" of the risk, prioritize the risk for its mitigation

4.5. Risk Mitigation

Risk mitigation options are evaluated through a comprehensive cost-benefit analysis. Response strategies are categorized into four approaches: Terminate, Take, Treat, or Transfer. Mitigation measures are regularly reviewed, updated, and designed to be both actionable and measurable.

When the selected risk response involves mitigation or transfer for a specific identified risk, the subsequent step is to review and enhance existing controls to address risks that exceed the defined risk appetite, as well as to identify and implement new or improved controls.

Identify controls.

New control activities are designed in addition to existing controls post assessment of risk exposure at current level to ensure that the risks are within the accepted risk appetite.

Control activities are categorized as Preventive or Detective based on their nature and timing:

- Preventive controls – focus on preventing an error or irregularity.
- Detective controls – focus on identifying when an error or irregularity has occurred. It also focuses on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

Evaluate Controls

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite.

Implement Controls

It shall be responsibility of the RMC to ensure that the risk mitigation plans for each function are in place and are reviewed regularly.

4.6. Risk Monitoring and reporting

Risk management processes are monitored through management controls, internal audits, and independent assessments. The outcomes of risk mitigation evaluations shall be reported to all relevant stakeholders to facilitate review, feedback, and ongoing oversight.

Given that an organization's risk exposure may evolve over time due to a continuously changing environment, the identified risks and their corresponding mitigation measures shall be regularly updated in the Risk Register by the designated "Risk Owners."

4.6.1. Risk Review, Governance and Independent assurance

The Three Lines of Defense model distinguishes among three groups (or lines) involved in effective risk management:

First Line of Defense	Second Line of Defense	Third Line of Defense
• Management Controls • Internal Controls	• Internal Financial Controls • Compliance reporting • Management reporting & review meetings	• Risk based internal Audits • External Audits • Independent Enterprise Risk Assessment reviews

Level 1: Functions that own and manage risks

As the first line of defense, Risk Owners are accountable for owning and managing risks within their respective areas. They are responsible for implementing corrective actions to address any process or control deficiencies.

Risk Owners must maintain effective internal controls and execute risk and control procedures on a day-to-day basis.

Risk Owners shall identify, assess, control, and mitigate risks, provide guidance in the development and implementation of internal policies and procedures, and ensure that all activities align with the organization's goals and objectives.

Risk Champions shall support Risk Owners in risk management activities within their designated areas of responsibility and are responsible for updating the Risk Register in accordance with inputs received from Risk Owners

Level 2: Functions and processes to oversee risks

The second line of defense is responsible for overseeing the overall effectiveness of risk management activities in conjunction with operational functions. This line of defense may consist of internal units or external agencies tasked with reviewing control efficiencies by means of:

- Periodic performance evaluations through MIS and management dashboards
- Ensuring compliance with the company's established policies and procedures
- Monitoring adherence to applicable laws and regulations
    - **Monthly Management Reviews-** Business functions are required to conduct self-assessments and present their results through dashboards to the respective function heads. Action plans addressing critical risks and issues identified must be developed and implemented with appropriate approvals from the leadership team. This review process shall also encompass emerging challenges and constraints relevant to each function.
    - **Compliance function:** The compliance function shall monitor specific risks, including non-compliance with applicable laws and regulations. Key issues and emerging risks identified shall be promptly reported to the Risk Coordinator.
    - **Internal Financial Controls Assessment:** Management shall conduct periodic reviews of internal financial controls to evaluate both the design and operating effectiveness of such controls across the organization. Identified gaps shall be communicated to the relevant functions, and appropriate remediation actions shall be defined and implemented to address these deficiencies. Key findings, along with the status of identified gaps and the progress of remediation efforts, shall be reported to senior management and the Board of Directors.
    - **Risk Management committee** shall oversee the overall effective risk management framework and monitor the key risks, mitigation measures, and implementation of action plan (covered in section 3 in detail)

Level 3: Functions that provide independent assurance

The third line of defense is responsible for conducting independent reviews of the company's risk management activities. This line of defense encompasses:

- Independent Risk Based Internal Audits
- External audits
- Independent periodic assessments of the risk management framework—including risk identification, evaluation, mitigation, and reporting—conducted by third-party consultants.

4.6.2. Risk Reporting & Communication

The outcomes of risk management activities shall be documented and communicated to relevant stakeholders throughout the organization. Timely communication of these outcomes enables stakeholders to make informed and appropriate decisions. Reporting of risk management activities is structured across three distinct levels:

First Line of Reporting

- Risk Owners shall provide quarterly reports to the ROC, detailing all identified risks, including emerging risks within their respective functions, along with the status of Early Warning Indicators.
- The ROC shall review and discuss key risks, emerging concerns, mitigation actions, and their status with the RMC. Any required adjustments to the risk mitigation plans shall be made accordingly and communicated to all relevant stakeholders by the ROC.

Second Line of Reporting

- The ROC shall convene RMC meetings at least twice annually, ensuring that no more than 210 days elapse between consecutive meetings.
- The ROC shall consolidate key risks arising from the discussions of the RMC and report them to the Board of Directors.

Third Line of Reporting

- ROC, on behalf of RMC, shall appraise the board on the key risks faced by the organization and the mitigation measures taken by the management.

(Refer Annexure for Risk Card)

5. Training, Awareness and Communication

To enhance knowledge and competency regarding the Enterprise Risk Management (ERM) framework at Shoppers Stop Limited, and to ensure that employees fully understand their roles and responsibilities in managing risks within their business units or functional areas, the following initiatives will be undertaken:

- Provide comprehensive training to the Board of Directors on the ERM framework and key risks to support effective oversight.
- The RMC will identify training needs and conduct targeted awareness sessions for relevant stakeholders, including Directors, Risk Owners, and Risk Champions.
- Incorporate risk management training into the employee induction program and maintain updated resources on the company intranet.
- Foster a risk-aware culture by disseminating periodic awareness communications to all employees.

6. Risk Culture

To successfully achieve its strategic goals and business objectives, Shoppers Stop Limited upholds its core values and actively promotes an open risk culture. This commitment includes organizing forums such as Town Halls and Risk Management meetings that provide employees with a platform to discuss existing and emerging risks. Leadership plays a pivotal role in shaping and reinforcing this culture, encouraging employees to proactively escalate risk-related concerns, particularly those that may conflict with business strategies. Such concerns are duly listened to and addressed by designated Risk Owners. Middle Management and Functional Managers ensure alignment with the company's Mission, Vision, strategies, and defined risk appetite. Additionally, the Board of Directors periodically monitors the prevailing risk culture and may instruct management to conduct risk culture surveys to assess and strengthen it further.

7. Annexure

7.1. Risk Register Format

Sr. No	Process	Risk Category	Risk Description	Root Cause	Risk Impact	Risk Likelihood	Risk Score	Overall Risk Grade (H/M/L)	Risk Mitigation Action Plans	Risk Owner	Action Plan Target Date	Action Plan Status

7.2. Risk Card for Identified Risk

R1:

Criteria	Score
Likelihood	
Impact	
Total	

What could go wrong

Strategic

Key drivers	Early warning indicators	Scenario Analysis

Mitigation plan	KRIs

1

7.3. Responsibility Accountability Consult Inform (RACI) Matrix

Activities	Responsibility	Accountability	Consult	Inform
Preparation/ updating of Risk Management Policy	Risk Coordinator	RMC		Board
Identification Functional / Divisional level risks and preparation of risk register	Risk Champions	Risk owners	Risk Coordinator	RMC
Facilitate to identify and monitor enterprise level risks	Risk Champions & Risk Owners, Risk Operating Committee	Risk Coordinator and RMC		Board
Define Mitigation plan	Risk Owners	Risk Operating Committee	Risk Coordinator	RMC
Implementation of Mitigation actions	Risk Owners	Risk Operating Committee	Risk Coordinator	RMC/ Board
Appraise Risk Management Committee on ERM Status	Risk Coordinator	Managing director	-	-
Appraise Board on ERM Status	Risk Coordinator	RMC	-	-

7.4. Escalation Matrix

Low		Moderate		High	
Immediate	**Periodic**	**Immediate**	**Periodic**	**Immediate**	**Periodic**
Risk Champions	Level 1: Risk Owners Level 2: Risk Coordinator	Risk Owners and Risk Champions	Level 1: ROC Level 2: Risk Coordinator	Level 1: Risk Owners and Risk Champions Level 2: CXO's	Level 1: ROC and RMC Level 2: MD, Vice Chairman and Chairman Level 3: BOD

7.5. SEBI Guidelines for composition of RMC

- The board of directors shall constitute a Risk Management Committee
- Risk Management Committee shall have minimum 3 members.
- Majority of members to be the members of board of directors,
- At least one independent director to be included in Risk Management Committee
- Meet at least twice a year and there should not be more than 210 days gap between two consecutive meetings.
- The board of directors defines the role and responsibility of the Risk Management Committee.
- Quorum of the meeting to be 2 or 1/3rds of total members of RMC, whichever is higher, Including at least 1 member of Board.