1. PREAMBLE:

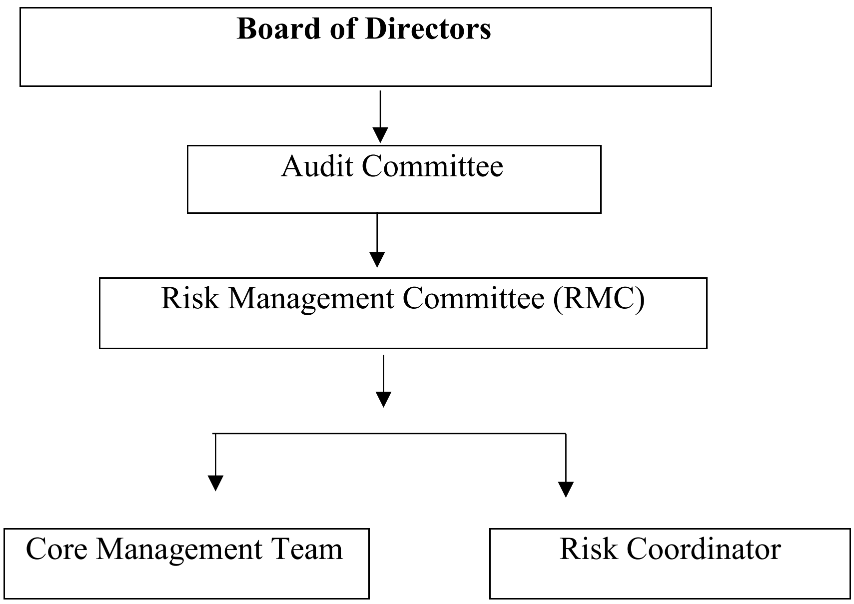
Risk is an integral part of the dynamic business environment. Risk is the probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action. Risk arises on account of uncertainty of occurrence and unknown consequences if the risk event were to occur. The degree of uncertainty or likelihood of occurrence and impact of the risk outcome combined together determine the magnitude of the risk.

2. OBJECTIVES:

The objective of this policy is to have a documented Risk Management Strategy in place, which provides a framework for identification, assessment, evaluation, mitigation and review of the risk categories on a periodic basis. This policy has been specifically designed, to achieve the following objectives:

a) Formulate a framework for identification of internal and external risks faced by company.
b) Measures for risk mitigation including systems and processes for internal control.
c) Define Business continuity plan.
d) Define framework for taking informed business decisions integrating risks to minimize adverse consequences of risks on business objectives.

3. RISK MANAGEMENT ORGANISATION STRUCTURE:



The roles & responsibilities of the above is as follows:

I. **Role and Responsibilities of Risk Management Committee:**

a) Formulate risk management policy including business continuity plan, monitor & oversee its implementation;
b) Frame and monitor Risk Management Plan;
c) Ensure methodology, processes and systems in place to monitor and evaluate risks;
d) Review risk management policy, every 2 years, considering changing industry dynamics and evolving complexity;
e) Appraise audit committee & board of directors about its discussions, recommendations and actions to be taken;
f) Maintain an aggregated view on risk profile and underlying business segments;
g) Appointment, removal and terms of remuneration of the Chief Risk Officer (CRO);
h) Constitute and monitor working of Core Management Team.

II. **Role and Responsibilities of Core Management Team:**

a) Identify and propose risks, evaluate criticality and formulate steps for mitigation;
b) Implement Risk Management Plan;
c) Review progress on mitigation action plan & its effectiveness;
d) Monitor movement of Key Risk Indicators (KRI) and endeavour to maintain them within the risk appetite;
e) In case any risk materialises, take appropriate actions as per the policy.

III. **Risk Co-ordinator**

a) Internal Audit incharge will act as Risk Co-ordinator and will report to CRO.
b) **Role and Responsibilities** –

i. Support Risk Owners in adhering to policy & Risk Management framework;
ii. Co-ordinate and schedule Core Management Committee meetings;
iii. Independently test the effectiveness of risk mitigation actions;
iv. Draft risk analysis, risk treatment and control mechanism in Risk Register;
v. Track actions proposed in the RMC and CMT meetings.

4. RISK MANAGEMENT FRAMEWORK:

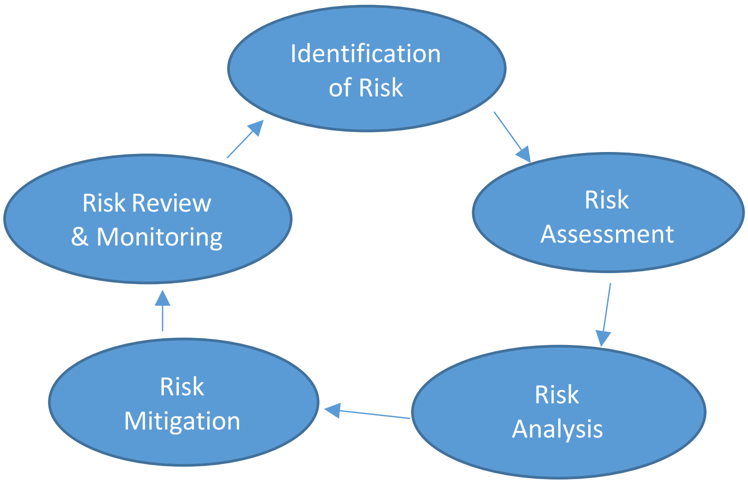
The Company has adopted Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2017 framework for its Enterprise Risk Management processes.

The Company's risk management framework sets the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management capability. Undertaking a periodic review to assess the effectiveness of the Company's risk management framework is necessary to ensure that the framework continues to evolve and meet the needs of the entity.

Integration of the Risk Management Framework with business objectives and monitoring effectiveness of the mitigation measures through a review of KRIs ensures effectiveness of the Risk Management Framework.

5. RISK MANAGEMENT PROCESS:

Risk Management is a continuous process that is accomplished throughout the life cycle of the organisation. Effective Risk Management covers risk management planning, early identification and analysis of risks, implementation of corrective actions, continuous monitoring & reassessment, and communication, documentation and coordination.



5.1.Risk Identification

The framework identifies internal and external risks faced by the Company including financial, operational, sectoral, sustainability (ESG related), information and cyber security risks. Strategic and operating risks are captured in risk register. Risk identification techniques are elaborated below:

Sources	Description
Internal Audit reports	Internal audit observations are evaluated to identify if any of those could pose a risk and mapped to the risk management framework wherever required
Peer Companies	On an annual basis, risks identified by the company and their mitigation measures are benchmarked with the risks and mitigation measures reported by peer entities in their Annual Reports to identify blind spots, if any and appropriate action taken to map them into the risk management framework wherever required
Whistle Blower mechanism	Learnings from investigations into whistle blower complaints also help to identify process gaps and risks.
Brainstorming	Perceived risks for a business are identified by key members of business teams through a brainstorming discussion every two years which acts as a platform to identify risks and opportunities
SWOT Analysis	During the preparation of the strategic plan, leadership team carries out a SWOT analysis and the weaknesses and threats identified during the said processes serve as inputs for risk identification
Scenario Analysis	Unprecedented or Unexpected events that have the potential to majorly impact the company's operations are evaluated by the Risk Management Committee on an annual basis

5.2.Risk Assessment & Analysis

Each of the identified risk is assessed on the twin factors of probability/ frequency and impact/ severity. The process of identifying the likelihood/frequency and impact/severity of risk events is a both quantitative and qualitative process of analysis. After finalizing the impact and the inherent risk is classified as under.

Risks	Description of Risk	Required Action
High	Event which can be tolerated but may have prolonged negative impact & extensive consequences	Continuous Active Management
Medium	Events which can be managed but requires additional resources and management efforts	Periodic monitoring
Low	Events, which can be managed/absorbed under normal operating conditions	No major concern

5.3.Risk Mitigation

Response to each of the identified risks are assessed in the context of Company's strategic direction and get suitably categorized into one of the following based on their linkage to the key strategic objectives of the Company:

a. Transfer
b. Avoid
c. Accept and absorb impact
d. Manage actively

Detailed mitigation action with timelines along with identified responsibilities for implementation are formulated for risks that are decided to be 'Managed Actively' as a response. Similarly, appropriate policies have been implemented to address the risk categories, mitigation whereof needs to be transferred.

Risks where the response is to either to "Accept and absorb impact" or "Avoid" are addressed as part of the company's strategy development framework in the context of the exposure management appetite that the Company may have for such risks.

5.4.Risk Review and Monitoring

A robust risk review and monitoring mechanism for the risk governance would be as follows:

a. Review with the Core Management Team and the CRO - All the risk registers to be reviewed annually in detail along with formulation of revised mitigation plan wherever required.
b. Review by the Executive Directors - Strategic and significant operating risks identified by each of the Risk owner will be reviewed annually in detail with the Executive Director responsible for operational oversight.

c. Review by the Risk Management Committee - The Risk Management Committee will identify every year, certain risks that are strategic from the corporate perspective which if not adequately addressed can have a major impact on the corporate performance. Such risks will be reviewed by the Risk Management Committee on an annual basis.
d. Review by the Audit Committee - Audit Committee shall review risk registers analysis presented by RMC.
e. Review by the Board of Directors - Update on mitigation measures against key risks will be submitted once in a year to the Board of Directors.

6. BUSINESS CONTINUTY PLAN:

Business continuity planning is the process involved in creating a system of either preventing or recovering effectively from the potential threats to company. The plan ensures that all assets of the company including people are protected and can function quickly in the event of a disaster. Effective implementation of Risk Management Policy can ensure continuity of business in all adverse scenarios. Business Continuity Planning shall be embedded in the Internal Controls and Core Management Team shall be responsible for laying out crisis response mechanism, communication protocols, and periodic training and competency building on crisis management.

The Core Management Team shall also conduct periodic disaster recovery mock drills to ensure that the organization is prepared to manage any crisis event quickly for business continuity.

7. POLICY REVISION:

Risks are ever changing in this volatile business environment and hence there is a need to periodically revisit the approach towards Risk management. Therefore, this policy shall be reviewed at least once in two years. Any revision to the policy shall be incorporated with the recommendation of Risk Management Committee & Audit Committee and approval of the Board of Directors.

****