Lux Industries Limited

This document captures the Risk Management Framework of Lux. It provides guidance to implement a consistent, efficient, and economical approach to identify, evaluate and respond to key risks that may impact business objectives.

Risk Management Policy

Effective Date: 14.11.2014

Approval Date: 14.11.2014

Version No.: 3.0

Reviewed on.: [01.11.2021]

Last revised on.: [01.11.2021]

Approved by: Board of Directors

Policy Owner: Managing Director

Subject: **Risk Management Policy**	Original Issue Date: 14.11.2014	Effective Date: 14.11.2014
	Revision Dates: 01.11.2021	Policy No.: 1

Governing Guideline/Policy	:	Companies Act 2013 and SEBI (LODR) 2015

BACK GROUND

This document lays down the framework for Risk Management at **Lux Industries Limited** (hereinafter referred to as the **'Company').** This document shall be under the authority of the Board of Directors of the Company, the Board has prepared this Policy with the objective to demarcate the role of Board, Audit Committee and the Risk Management Committee for the purpose effective Risk Management, it seeks to identify risks inherent in the business operations of the Company and provide guidelines to define, measure, report, control and mitigate the identified risks.

OBJECTIVE

The objective of Risk Management at Lux Industries Limited is to create and protect shareholder value by minimizing threats or losses, and identifying and maximizing opportunities. An enterprise-wide risk management framework is applied so that effective management of risks is an integral part of every employee's job.

Strategic Objectives

1. Providing a framework that enables future activities to take place in a consistent and controlled manner
2. Improving decision making, planning and prioritization by comprehensive and structured understanding of business activities, volatility and opportunities / threats
3. Contributing towards more efficient use / allocation of the resources within the organization
4. Protecting and enhancing assets and company image
5. Reducing volatility in various areas of the business
6. Developing and supporting people and knowledge base of the organization.
7. Optimizing operational efficiency

REGULATORY

Risk Management Policy is framed as per the following regulatory requirements:

1. **Section 134(3)(n)**
   There shall be attached to financial statements laid before a company in general meeting, a report by its Board of Directors, which shall include –

   "(n) a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company."

2. **Section 177(4)(vii)**
   Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include, -

   "(vii) evaluation of internal financial controls and risk management systems."

3. **Schedule IV (II) (1) and (4)**
   The independent directors shall:
   (i) help in bringing an independent judgment to bear on the Board's deliberations especially on issues of strategy, performance, ***risk management,*** *resources, key appointments and standards of conduct;*

   (ii) satisfy themselves on the integrity of financial information and that financial controls and ***the systems of risk management*** *are robust and defensible;*

A. SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015

Regulation 4(2)(f)(ii)(1) and (7)

Key functions of the board of directors-

i. *Reviewing and guiding corporate strategy, major plans of action, risk policy, annual budgets and business plans, setting performance objectives, monitoring implementation and corporate performance, and overseeing major capital expenditures, acquisitions and divestments;*
ii. *ensuring the integrity of the listed entity's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.*

Regulation 17(9)(a) and (b)

i. *The listed entity shall lay down procedures to inform members of board of directors about risk assessment and minimization procedures.*
ii. *The board of directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.*

Regulation 18 read with Para A of Part C of Schedule II

The role of the audit committee shall include the evaluation of internal financial controls and risk management systems.

d. **Regulation 21 read with Para C of Part A of Schedule II**

The board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit [such function shall specifically cover cyber security].

Provided that the role and responsibilities of the Risk Management Committee shall mandatorily include the performance of functions specified in Part D of Schedule II.

e. Para C of Part D of Schedule II

The role of the committee shall, inter alia, include the following:

(1) To formulate a detailed risk management policy which shall include:
(a) A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
(b) Measures for risk mitigation including systems and processes for internal control of identified risks.
(c) Business continuity plan.

The Company, being listed, is required to adhere to the Companies Act, 2013 and SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (SEBI LODR). Where any stipulation is common between the regulations, more stringent of the two shall be complied with.

DEFINITIONS

"Audit Committee" means Committee of Board of Directors of the Company constituted in accordance with the provisions of Section 177 of the Companies Act, 2013 ("Act") read with the Regulation 18 of the SEBI LODR.

"Board of Directors" or "Board" in relation to a Company, means the collective Body of Directors of the Company constituted in accordance with the provisions of Section 2(10) of the Act, read with the Regulation 2(1)(d) of the SEBI (Listing Obligations and Disclosure Requirements) 2015

"Policy" means Risk Management Policy framed and adopted by the Board of and reviewed by the Board and Risk Management Committee of from time to time.

.

"Risk Management Committee" or **"RMC"** is a Committee constituted in accordance with the provisions of Regulation 21 of SEBI LODR and other applicable laws.

"Risk Management System" or **"Risk Management"** is the process of identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of the identified Risks.

"Risk Management Plan" is a written document prepared by the management of the Company that details the organization's risk management process including the foreseeing of risks, estimating impacts, and define responses to such risks.

POLICY STATEMENT

Before proceeding to the policy attention is drawn to the roles that the Board and Risk and Audit Committee are required to play under the above regulations governing Risk Management:

The Board's role under both the regulations is to ensure framing, implementing and monitoring risk management plan, having in place systems for risk management as part of internal controls with duty being cast upon Independent Directors to bring unbiased angle to the Board's deliberations on making risk management systems more robust.

Risk and Audit Committee's role is evaluation of the risk management systems.

This policy shall complement the other policies of Company in place e.g. Related Party Transactions Policy, to ensure that the risk if any arising out of Related Party Transactions are effectively mitigated.

BOARD PRINCIPLES

The Board has to review the business plan at regular intervals and develop the Risk Management Strategy which shall encompass laying down guiding principles on proactive planning for identifying, analyzing and mitigating all the material risks, both external and internal viz. Environmental, Business, Operational, Financial and others. Communication of Risk Management Strategy to various levels of management for effective implementation is essential.

Risk Identification is obligatory on all vertical and functional heads who with the inputs from their team members are required to report the material risks to the CRO along with their considered views and recommendations for risk mitigation.

Analysis of all the risks thus identified shall be carried out by CRO through participation of the vertical/functional heads and a preliminary report thus finalized shall be placed before the Risk Management Committee.

ROLE OF THE CRO

The CRO has responsibility for identifying, assessing, monitoring and managing risks. Primarily, the CRO is also responsible for tracking and identifying any material changes to the Company's risk profile and ensuring, with recommendations and approval of the Risk Management Committee (RMC) and the Board, the risk profile of the Company is updated to reflect any material change.

Implementation of the risk management system and day-to-day management of risk is the responsibility of the CRO, with the assistance of senior management, as required.

The Chief Risk Officer is required to report to the Board as to the effectiveness of the Company's management of its top 10 critical business risks on a regular basis.

The Chief Risk Officer shall be responsible for tracking and ensuring that all the action plan devised for identified risks are being implemented within stipulated timelines.

ROLE OF THE HEADS OF THE DEPARTMENTS

Heads of Departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning and report to the CRO. Heads of Departments are required to provide updates on status of action plans devised for risks identified in their respective areas (action taken report) periodically to the CRO.

RISK CATEGORIES AND PROFILE

The Company considers that any risk that could have a material impact on its business should be included in its risk profile. All the identified risks shall be categorized under the following categories:

1. Strategic Risks: Risk of loss resulting from business factors. These adversely affect the achievement of strategic objectives and may impair overall enterprise value.

2. Operational Risks: Risk of loss resulting from inadequate or failed processes, people and information systems,

3. Reporting Risks: Risks of inadequate internal or external reporting due to incorrect financial and non-financial information in the reports.

4. Compliance Risks: Risk of loss resulting from legal and regulatory factors.

5. IT-related Risks: Risk of technological challenges and other cyber security risks.

S.no.	Risk Category	Risk Areas
1	Strategic Risks	• Business Risks • Competition Risks • Business Contingency/ Continuity Risks including natural disasters • Reputation Risks • Sustainability Risks • Political Risks

2	Operational Risks	• Quality Risks • Cost Risks • Raw Material Risks • Internal Control Risks • Talent Attrition Risks
3	Reporting Risks	• Financial risk including liquidity, forex risk, credit risk • Realization Risks
4	Compliance Risks	• Legal Risks • Health, Safety and Environmental Risks
5	IT Risks	• Technological Risks including hardware and software failure, human error, spam, viruses and malicious attacks • Cyber Security Risks such as ransomware, phishing, data leakage, hacking, insider threats

RISK ASSESSMENT

Risk assessment allows the company to consider the extent to which potential events might have an impact on achievements of its objectives. Hence, Management shall assess events from two perspectives – **likelihood and impact.**

Likelihood Rating: Determination of risk Occurrence

Risk Measurement Score	Classification	Likelihood
1	Rare	Risk has not occurred; can occur in exceptional cases
2	Unlikely	Risk has occurred remotely in the past; not expected but may happen
3	Possible	Periodic occurrence; event has possibility to occur in the year
4	Likely	Annual occurrence; likely for event to occur
5	Utmost Certain	More than once per year; almost certain for event to occur

IMPACT RATING

	Consequence Description				
Impact	**Profit (EBITDA) Reduction**	**Impact on Revenue**	**Health and Safety**	**Community, Government, Reputation, Media**	**Legal**
1- Negligible	-	-	No medical treatment required	Minor, adverse local public and media	Minor legal issues

				attention	
2 - Minor	< XX Cr.	< XX Cr.	Objective but reversible disability requiring hospitalization	Attention from media; heightened concern by local community	Noncompliance and breaches of regulation
3- Moderate	Between XX Cr. – XX Cr.	Between XX Cr. – XX Cr.	Moderate irreversible disability or impairment to one or more persons	Criticism by national government	Serious breach of regulation with investigation or report to authority with prosecution or moderate fine possible
4 - Major	Between XX Cr. – XX Cr.	Between XX Cr. – XX Cr.	Single fatality or severe, irreversible disability to one or more persons	Significant adverse national media or public or national government attention	Major breach of regulation; major litigation
5 - Severe	>XX crores	>XX crores	Multiple fatalities or significant, irreversible effects to >50 persons	Serious public or media outcry; international coverage	Significant prosecution and fines; very serious litigation including class actions

RISK MANGEMENT PROCESS

The key **risk management process** would broadly include

1. Risk Identification:

- Assessment of organization's exposure to uncertainty which requires in-depth knowledge of the organization, market, economic, legal, cultural, regulatory, technological environment in which it exists
- Risk identification shall be approached in a methodical way to ensure that all significant activities within the organization have been identified
- Primary responsibility of identification of risks lies with respective HoDs however, the same can also be suggested by CRO or RMC

2. Risk Categorization:

- All identified risks shall be categorized under defined category buckets i.e., Strategic, Operational, Reporting, Compliance and Technology
- CRO and RMC are responsible for categorization of risks

3. Assessment of identified risk:

- Risk assessment allows the company to consider the extent to which the potential event might affect the company
- Risk assessment should be performed from two perspectives – likelihood and impact
- CRO and RMC are responsible for assessment of risks in consultation with respective HoDs

4. Risk mitigation:

- Developing strategies / alternatives to reduce or treat the potential risks
- The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way
- CRO and RMC are responsible for assessment of risks in consultation with respective HoDs

5. Risk reporting and disclosures:

- Risk Management Committee shall report the risks along with assessment and mitigation plans to the Board within stipulated timelines

6. Monitoring of the risk mitigation efforts:

- Risk Management Committee shall monitor all aspects of an identified risk on a regular basis as the risk exposure may undergo changes from time-to-time due to continuously changing environment
- CRO and RMC are responsible for monitoring of risk mitigation efforts in consultation with the Board

7. Integration with strategy and business plan:

- Risk Management Committee shall be responsible for regular policy reviews and review standard performance to identify opportunities for improvements
- Chief Risk Officer to ensure that the measures adopted resulted in what was intended

RISK REGISTERS

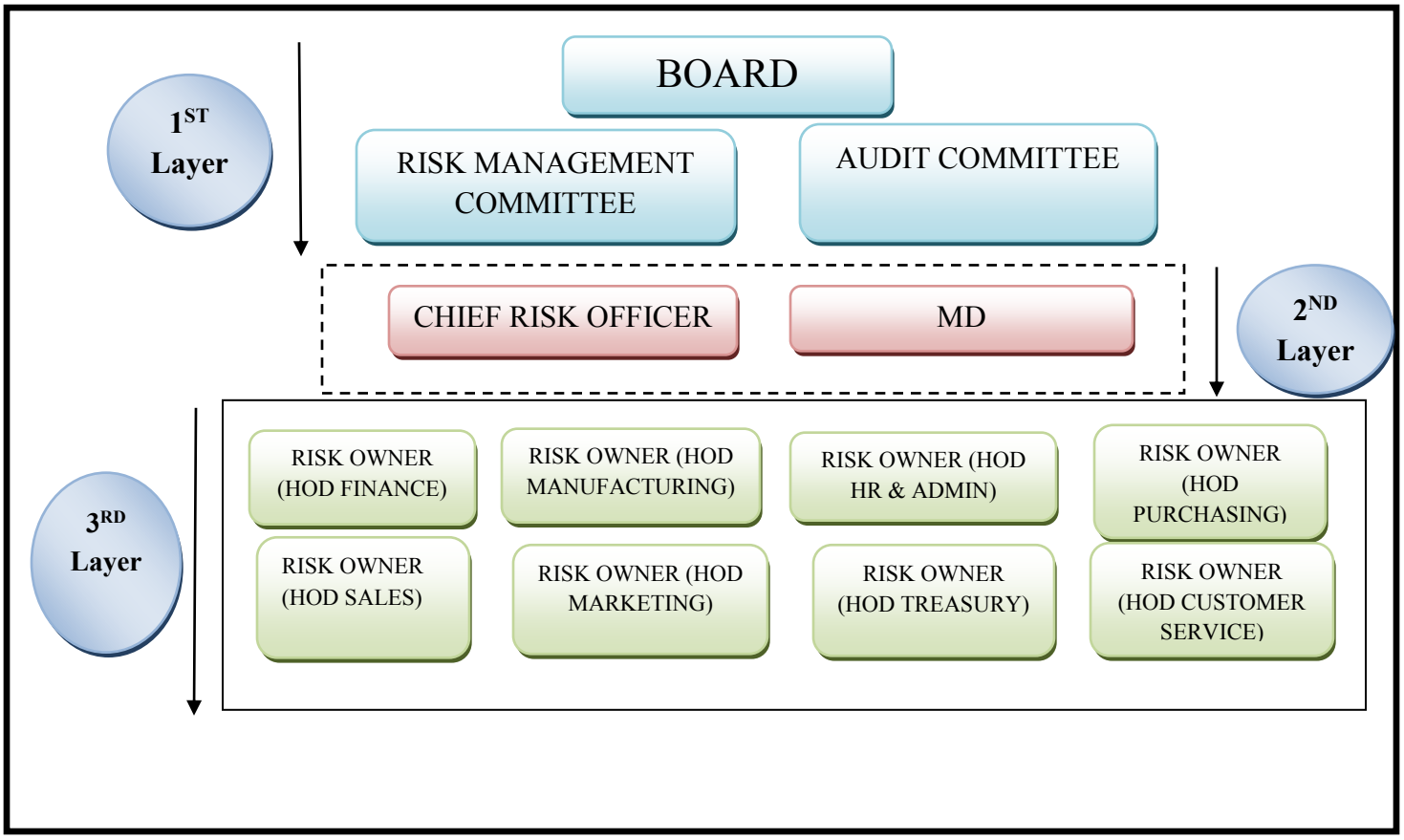
Centralized Risk registers along with mitigation / action plans shall be maintained. (Refer Annexure 1 for Risk Register format) Risk registers to be duly updated on a periodic basis by Risk Owners (HoDs) for their respective areas.

GOVERNANCE STRUCTURE

The following risk governance structure shall establish clear allocation of roles and responsibilities for management of risks on a day to day basis.

Line of reporting:

1. Risk Owners shall report to CRO on quarterly basis and track material changes
2. CRO shall report to the Risk Management Committee from time to time to identify key risks which need to be reported to the Board
3. CRO and Risk Management Committee shall apprise the Board on key risks faced by the organization twice in a year along with risk assessment and mitigating action plans
4. The Company Secretary shall act as Secretary to Risk Management Committee (RMC) for the purpose of convening of RMC Meeting and recording its minutes periodically.



The following responsibilities must be carried out by Risk Management Committee in consultation with the Board of Directors:

1. To recommend the risk appetite of the organization for overseeing that the Company is taking appropriate measures in achieving prudent balance between risk and reward in both ongoing and new business activities.
2. To oversee that the Company has implemented an effective ongoing process and risk awareness culture in the organization to identify risk, to measure its potential impact and then to activate what is necessary to pro-actively manage these risks
3. RMC to obtain suggestions and approvals from the Board for the risk appetite of the organization
4. To oversee that the risk awareness culture is pervasive throughout the organization.
5. To review the risk bearing capacity of the Company in light of its reserves, insurance coverage, guarantee funds or other such financial structures.

ROLES & RESPONSIBILITIES OF RISK MANAGEMENT COMMITTEE

Risk Management Committee shall meet at least **twice in a year** to fulfil following roles & responsibilities

Roles:

- To access the Company's risk profile and key areas of risk in particular.
- To recommend the Board and adoption of risk assessment and rating procedures.
- To articulate the Company's policy for the overnight and management of business risks.
- To examine and determine the sufficiency of the Company's internal processes for reporting on and managing key risk areas. To assess and recommend the Board acceptable levels of risk. To develop and implement a risk management framework and internal control system. To review the nature and level of insurance coverage.
- To have special investigations into areas of corporate risk and breakdowns in internal control.

- To review management's response to the Company's Auditors' recommendations those are adopted.
- To report the trends on the Company's risk profile, reports on specific risks and the status of the risk management process to Board of Directors twice in a year.
- To assess the Company's risk profile and key areas of risk in particular.
- To recommend the Board and adoption of risk assessment and rating procedures.
- To articulate the Company's policy for the oversight and management of business risks.

Responsibility:

1. To exercise oversight of management's responsibilities and review the risk profile of the organization to ensure that risk is not higher than the risk appetite determined by the board.
2. To assist the Board in setting risk strategies, policies, frameworks, models and procedures in liaison with management and in the discharge of its duties relating to corporate accountability and associated risk in terms of management assurance and reporting and that infrastructure, resources and systems are in place for risk management is adequate to maintain a satisfactory level of risk management discipline.
3. To review and assess the quality, integrity and effectiveness of the risk management systems and ensure that the risk policies and strategies are effectively managed. Also, to review and assess the nature, role, responsibility and authority of the risk management function within the Company and outline the scope of risk management work.
4. To ensure that a systematic, documented assessment of the processes and outcomes surrounding key risks is undertaken at least annually for the purpose of making its public statement on risk management including internal control.
5. To oversee formal reviews, processes and procedures of activities associated with the effectiveness of risk management and internal control processes. A comprehensive system of control should be established to ensure that risks are mitigated, Company's objectives are attained, and financial results are always maintained at an optimal level
6. To provide an independent view of the information presented by the management on corporate accountability and specifically associated risk, also taking account of reports by the Audit Committee to the Board on all categories of identified risks facing by the Company.
7. To review issues raised by Internal Audit that impact the risk management framework.
8. Perform other activities related to risk management as requested by the Board of Directors or to address issues related to any significant subject within its term of reference.
9. The Risk Management Committee (RMC) shall ensure implementation of this policy and periodically assess risks and review key leading indicators in this regard. All categories of Risks and their mitigation plans along with risk assessment would be reviewed by RMC on a half yearly basis.
10. The RMC shall half yearly review and approve the Enterprise Risk Management Framework of the Company. The RMC shall twice in a year review the risk management processes and practices of the Company in consultation with the Chief Risk Officer.
11. The RMC shall evaluate significant risk exposures of the Company and assess management's actions to mitigate the exposures in a timely manner (including one-off initiatives, and ongoing activities such as business continuity planning and disaster recovery planning & testing).
12. The RMC shall evaluate risks related to cyber security and ensure that management initiated appropriate procedures to mitigate these risks in a timely manner.
13. The RMC will coordinate its activities with the Audit Committee in instances where there is any overlap with audit activities (e.g. internal or external audit issue relating to risk management policy or practice).
14. The RMC shall make regular annual reports to the Board, including with respect to risk management and minimization procedures.

15. The RMC shall have access to any internal information necessary to fulfill its oversight role. The RMC shall also have authority to obtain advice and assistance from internal or external legal, accounting or other advisors.
16. The role and responsibilities of the Risk Management Committee shall include such other items as may be prescribed by applicable law or the Board in compliance with applicable law, from time to time.
17. RMC To formulate a detailed risk management policy which shall include:
    a. A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (specifically, Environmental, Social and Governance related risks and impact), information and cyber security risks
    b. Measures for risk mitigation
    c. Systems for internal controls and
    d. Business contingency plan.

BUSINESS CONTINUITY PLAN (BCP)

Introduction & objective

Risk that cannot be envisaged or intensity of which cannot be envisaged may lead to Disaster. Accordingly, an effective risk management plan should also have provision with respect to dealing with Disaster to be able to continue with the operations with minimum disruption.

A 'Business Continuity Plan' (BCP) is a systematic guideline that details the probable impact of an instance of Disaster, the ideal response to such situations, and the recouping mechanism to bring the business function back on track with minimal disruption. It involves each key stakeholder of the business and how they should act /& react to the occurrence of a Disaster. The ultimate aim of BCP is to ensure that the personnel and properties of the Company are protected on and after the occurrence of a Disaster.

Definition

"**Disaster**" *means a catastrophe, mishap, calamity or grave occurrence in any area, arising from natural or man-made causes, or by accident or negligence which results in substantial loss of life or human suffering or damage to, and destruction of, property, or damage to, or degradation of, environment, and is of such a nature or magnitude as to be beyond the coping capacity of the community of the affected area." - Disaster Management Act, 2005*

Kinds of Disaster

An emergency event poses a host of challenges wherein a business can not function in the normal course and requires substantial adjustments in operation including personnel. The event could be of 2 categories;

- Natural events (force majeure)
    - fire, flood, earthquake, tornado, pandemic etc
- Man-made events
    - Terrorism, cyber-attacks, power outage, etc.

Disaster response team

There needs to be a group of employees at each business location depending upon the scale of operations and the number of people employed at each location. There could be involvement of external stakeholders as well depending upon the nature of the event.

The response team should be trained periodically to enable them to respond appropriately to the occurrence of a risk event.

The company shall have a medical response team, contacts with nearby hospitals, electric back-up for power outage, fire and safety equipments, insurance for personnel at every business location, back-up servers for data recovery in case of cyber-attacks, etc. as a part of its readiness for battling a Disaster.

External Communication

The communication of the occurrence of a risk event should be communicated with at most care and proper medium to ensure that the external stakeholders are given information on a timely basis to avoid any kind of speculation. There needs to be a proper line of communication with the responsibility lying with key people of the response team.

Designated Contact list

There should be a designated contact list for communications on the occurrence of a risk event. Also, the contact list shall be updated on a timely basis. It shall include:

- Internal staff and people listed as emergency contact
- Emergency services (Police, Fire & Rescue, Ambulance, etc.)
- External stakeholders (Media, Investors, Regulators, etc.)
- Insurance providers

Periodic review including mock-drills

The entire activities and the plan once framed need to be evaluated on a periodic basis to ensure that the established framework is reliable and fool-proof. There should also be conducted mock-drills of disaster response like for fire, etc., and the effectiveness of evacuation, response, and the shortcomings if any in the plan. This would also help in updating the existing framework based on real experiences.

Turnaround Plan

The plan shall include the activities that should be carried out for recovery after a risk event/disaster has disrupted the business. It shall define those activities depending upon the type of risk event/disaster and the scale of loss that happened. The aim is to minimise the financial loss and put the operations back on track at the earliest time possible.

INTEGRATION OF RISK MANAGEMENT STRATEGY

Company's risk management strategy is to be integrated with the overall business strategies of the organization and its mission statement to ensure that its risk management capabilities aide in establishing competitive advantage and allow management to develop reasonable assurance regarding the achievement of the Company's objectives.

PENALTIES

The penalties are prescribed under the Companies Act, 2013 **(the Act)** under various sections which stipulate having a Risk Management Framework in place and its disclosure.

Section 134 (8) (dealing with disclosure by way of attachment to the Board Report): If a company contravenes the provisions of this section, the company shall be punishable with fine which shall not be less than fifty thousand rupees but which may extend to twenty-five lakh rupees and every officer of the company who is in default shall be punishable with imprisonment for a term which may extend to three

years or with fine which shall not be less than fifty thousand rupees but which may extend to five lakh rupees, or with both.

There are other provisions of the Act as well as SEBI Act which stipulate stiff penalties. Therefore, this Policy prescribes that violation of the provisions applicable to Risk Management Framework is something the Company cannot afford to risk.

REVIEW

This policy shall evolve by review by the Risk Management Committeeand the Board from time to time as may be necessary.This policy will be communicated to all vertical/functional heads and other concerned persons of the Company.