National Aluminum Company Limited

RISK MANAGEMENT POLICY

DOCUMENT CONTROL

Version 1.0	
Authorized By:	Date: 29/*09/2024*
Approved By:	Date: 29/*09/2024*

REVISION RECORD SHEET

Version	Date	Approval
1.0		

Table of Contents

INTRODUCTION

National Aluminium Company Limited (referred to as "**NALCO**" or the "Company") recognizes the operational complexities it faces within a dynamic business landscape. As the industry continues to evolve and regulatory frameworks undergo consistent changes, it is imperative for the Company to proactively address potential risks and ensure effective risk management practices are in place.

NALCO is committed to effectively managing operational, financial, and other risk in the context of business strategies and with a view to achieving a balance between acceptable levels of risk and reward. NALCO recognizes that risk management is of concern to all levels of the business and requires a risk management policy and process involving all personnel, with reporting structures to the Board.

NALCO has laid down a Risk Management Policy (*hereafter referred to as the* "***Policy***") that details therein guidelines for implementation of Enterprise Risk Management (*hereafter referred to as* "***ERM***") framework across the Company. The policy supports the Company's endeavor to design, implement, monitor, review, and continually improve its risk management practices.

This Policy has been developed to promote risk management within the Company, with an aim of enabling the achievement of strategic objectives. This document also provides an overview of the Company's Risk Governance structure and illustrates the roles and responsibilities of various stakeholders within it. It majorly encompasses the following elements:

- Policy Objectives
- Risk Governance Structure
- Risk Management Roles and Responsibilities

The Risk Management policy shall be read with the Enterprise Risk Management Framework, which lists down the detailed risk management process to be followed to identify potential risks and ensure timely risk response. The detailed guidance on risk management for the Company can be found in the ERM Framework.

1. Purpose

The purpose of this document is to define the requirements around Enterprise Risk Management and sets out the objectives and accountabilities for risk management within the Company such that it is structured, consistent and effective, to facilitate and improve the Company's risk management capabilities in a dynamic business environment.

2. Regulatory Requirements

The Companies Act 2013, and SEBI LODR (hereafter referred to as "Listing Regulations"), 2015 and as amended from time to time, have incorporated various provisions in relation to Risk Management Policy.

The provisions of Section 134(3)(n) of the Companies Act, 2013 necessitate that the Board's Report should contain 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.

The provisions of Part-D of Schedule II of SEBI Listing regulations, require that the Risk Management Committee develop a detailed risk management policy for the listed Company, monitor and oversee its implementation and evaluate adequacy of risk management systems, and periodically review the risk management policy at least once in two years, considering industry dynamics and evolving complexity.

3. Scope

The policy shall apply to all business units of National Aluminium Company Limited. This policy shall apply consistently across all levels of the Company, including the management, Business Units, key corporate functions, operations, projects, employees, contractors, business partners, and/or individuals directly/indirectly associated with the enterprise. All employees of the Company are required to adhere to this policy.

4. Objectives

The Risk Management Policy provides a structured and disciplined approach to the Risk Management process to facilitate informed decision-making on risks, with specific objectives mentioned below:

- Provide guidelines of risk management and approach adopted by the Company for management.
- Provide a strategic framework for NALCO’s risk management process in alignment with the strategic objectives including the risk governance structure for effective risk management.
- Promote an effective risk management system that supports the Company’s growth strategy and business objectives.
- Support the achievement of the Company’s mission, vision, and strategic priorities in line with its core values, through risk-informed decision-making across the Company.
- Integrate risk management in the culture and strategic decision making across the Company.
- Establish a structured processes for early identification, assessment, risk response, monitoring, and reporting on risks arising out of internal as well as external factors.
- Identify and diligently pursue both new and existing opportunities in alignment with the Company's defined risk appetite and tolerance levels.
- Establish a process to identify and assess risks that may impact the business continuity of the Company and define response recovery plans for such risks.
- Establish and guide risk governance by providing clarity on the roles and responsibilities in relation to risk management.
- Facilitate compliance with the applicable regulatory requirements related to risk management and reporting

5. Risk Management Policy Statement

The Company is committed to establishing a robust mechanism for proactive risk management, which is based on the following underlying principles:

- The Company shall encourage and strengthen the accountabilities, ownership, and responsibilities with respect to risk management across all levels and activities of the Company.

- The Company will align and integrate varying views on risk management and review and monitor a uniform risk management framework across the Business Units, key corporate functions, and projects of the Company.

- The Company aims to identify, monitor, and take preventive action to manage or treat risks that may impact its strategic objectives and continuity of its operations.

- The Company endeavors to create and foster risk awareness across the Company, through continuous education and training on risk management.

- The Company aims at inculcating risk appropriate attitudes and behaviors by integrating Risk Management as a key responsibility area for employees and the compliance to risk management policy and frameworks as a KPI for the functional heads/senior management team.

6. Risk Management Governance Structure

The responsibility for risk management is shared across the Company. The company has established three pillars of risk management responsibilities in its Governance structure, that cascades the scope of activities to senior management and all employees, across all operating entities of the Company.

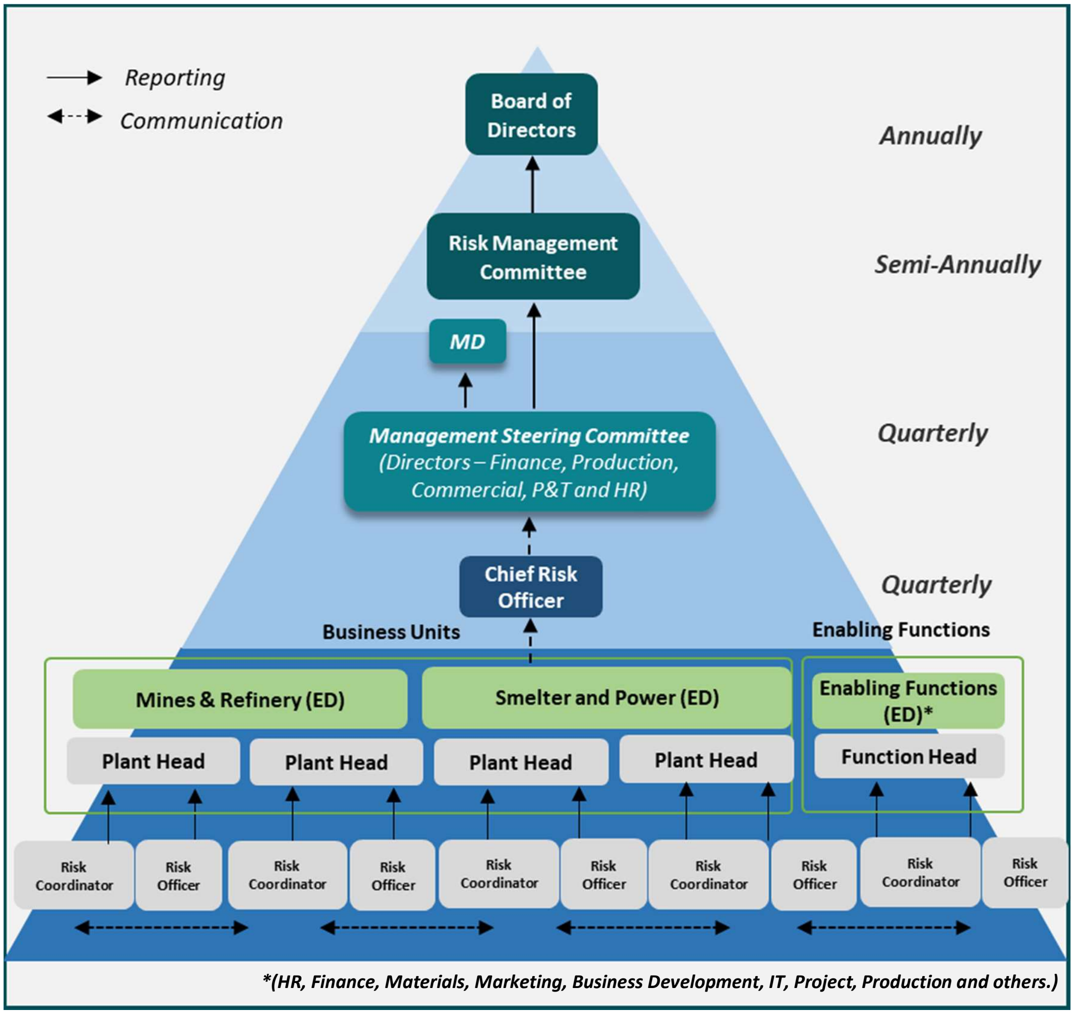

Figure 1: Risk Management Governance Structure

7. Risk Management Responsibilities

A. Risk Governance and Oversight

Risk governance and oversight are critical components of ensuring the long-term success and sustainability of the organization. By establishing a robust framework, defining risk appetite, and setting clear risk management policies, the organization can effectively identify, assess, and mitigate risks. Through proactive risk governance and oversight, the organization can safeguard stakeholder interests and enhance decision-making processes.

7.1.1 Board of Directors

The Board of Directors (hereafter referred to as the "Board") will play a critical role in overseeing the deployment of risk management process throughout the Company and setting the tone and culture towards effective risk management by affixing risk appetite, formulating high level objectives and strategy setting. The Board will meet quarterly to review the key residual risks, including strategic and emerging risks as per prioritization criteria, and status of associated response plans. The Board will undertake a comprehensive evaluation of the Company's risk portfolio to assess its alignment with the Company's risk tolerance.

The key roles and responsibilities of the Board of Directors are as follows:

- Approve the Risk Management Policy and Procedures document
- Review and approve the risk appetite for the Company
- Review and approve the Company's risk profile against the risk appetite
- Evaluate the effectiveness of risk management systems
- Review the risk exposure of the Company, including strategic and emerging risks and associated risk response plans.
- Review and approve adequacy and effectiveness of business risk management and risk disclosures in adherence to regulatory requirements
- The Board of Directors may assign additional responsibilities to the Risk Management Committee with an aim to strengthen the risk culture across the organization.

7.1.2 Risk Management Committee

The Risk Management Committee (hereafter referred to as "RMC" or "Committee") shall meet twice in a year, with a maximum gap of 210 days between any two consecutive meetings and will oversee the adequacy of risk management systems as per SEBI LODR Regulations, 2015. The RMC shall be entrusted with the responsibility to assist the Board in framing policy, guiding implementation, monitoring, and reviewing the effectiveness of policy. The RMC will act as a forum to discuss and manage key residual risks on a quarterly basis and appraise the Board on risk management.

The roles and responsibilities of the RMC are as follows:
The Committee shall have the following roles and responsibilities (as read with Roles and responsibilities of Risk Management Committee (RMC) under Part-D of Schedule II of SEBI (LODR):

- Advise the Board on the effectiveness of the risk management systems at least annually.
- Keep the Board informed about the nature and content of RMC discussions, recommendations, and actions to be taken.
- Review the risk management policy which shall include a framework for,
  a) Identification of internal and external risks faced by the Company, including financial, operational, sectoral, sustainability (including, ESG related risks), information, cyber security risks or any other risk as may be determined.
  b) Identification and implementation of risk response measures including systems and processes for internal control of identified risks.
  c) Business continuity plan.
- Monitor, review and recommend improvements in the risk management procedures, which shall include:
  a) Updates to risk and appetite and assessment scales;
  b) Procedures for identification of risks and associated risk responses;
  c) Processes for risk assessment.

- Review the key risks for the enterprise twice in a year, with a maximum gap of 210 days between any two consecutive meetings.
- Approve disclosures related to risk matters.
- Assess the risk culture and guide the management to foster and strengthen the risk culture.
- Propose enhancements to the Risk Management system, including those required in adherence to changes in regulatory requirements and guide the Risk Management function.
- Periodically review the risk management policy, at least once in two years, and recommend to Board for approval.
- Review the appointment, removal, and terms of remuneration of the Chief Risk Officer.
- Seek information from any employee, obtain outside legal or other professional advice and secure attendance from outsiders with relevant expertise, if considered necessary.
- The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board of Directors.

B. Risk Infrastructure and Management

The Risk Governance and Oversight function played a pivot role in framing the Risk Management Policy and Procedures. The next two levels of risk responsibilities, namely Risk Infrastructure and Risk Ownership, are shared by the key executives and working officials of the Company. The roles and responsibilities for teams constituting the Risk Infrastructure function as per the risk governance structure are as elaborated below.

7.2.1 Management Steering Committee

The Management Steering Committee (hereafter referred to as "MSC") is a sub-committee assisting the RMC. The MSC shall assist the Board and RMC in fulfilling its oversight responsibility for the risk management process and systems within the Company.

Composition

The MSC shall comprise of the Company's senior management. The members of the MSC include the following:

- Director (Finance)
- Director (Production)
- Director (Commercial)
- Director (P&T)
- Director (HR)

The GGMs and Head of Departments (HoDs) of the respective departments or their nominated risk officers may be invited by the MSC to present their respective key residual risks and associated risk response plans as required. They may be invited to attend part or all MSC meetings as appropriate.

The identified risks will be presented to the Managing Director (MD) prior to their discussion within the Risk Management Committee (RMC). The MD's guidance and approval may be taken in matters related to amendments in policies and procedures, risks requiring intervention of the MD or Board of Directors (in terms of strategic and investment related decisions for the Company), additional resource/budgetary allocation or appointment of external consultants, among other activities related to risk management for the Company.

Quorums

A quorum for the transaction of business at any meeting of the MSC shall consist of a majority of members. Actions of the Committee shall be taken by majority vote of the members in attendance. Each member shall have one vote on each matter before the MSC.

Meetings

- The MSC shall meet on a quarterly basis during the year.
- All or any members may participate in a meeting by video conferencing or by other audio-visual means. A member so participating is deemed to be present in person at the meeting and shall be counted for the purpose of quorum at the meeting of the MSC.
- The Chief Risk Officer shall convene the quarterly MSC meetings and present risk management matters to the MSC.
- The Chief Risk Officer shall be supported by the Secretary to compile and circulate the agenda and papers for the MSC meetings and minutes subsequent to the meeting.

Roles and Responsibilities

The roles and responsibilities of the MSC are as follows:

- Review the existing risk management process and documentation. Deliberate on the establishment, operations, and continuous improvement of the risk management structure.
- Help establish limits and controls on risk appetite for the Company in consultation with the Finance department and respective departments.
- Approve and convey, in consultation with the MD, strategies, procedures, and guidelines that embed risk assessment and response to risk considerations into
  - I. Planning processes;
  - II. Strategy development and execution, and
  - III. Capital authorization requests, if required.
- Review risks associated with proposed capital investments prior to investment decisions.
- Monitor and review the key enterprise risks for the Company and evaluate the appropriateness of risk response plans for key residual risk(s) on a quarterly basis.
- Set up mechanisms to identify the various scenarios that may adversely impact the business continuity of the Company and evaluate the Company's readiness in responding to such scenarios.
- Review key residual risk(s), associated response plans, and the changes in risk rating. Thereafter, the MSC shall prioritize the key residual enterprise risks and associated response plans to be reported to the RMC.
- Carry out any other activities as may be required or deemed necessary in this regard.

7.2.2 Chief Risk Officer

The Chief Risk Officer (CRO) shall assist the Board and the Audit and Risk Management Committee in review and oversight responsibilities related to Risk Management. The CRO shall facilitate the risk management processes within the Company and support the management in fostering and developing a risk aware culture.

The roles and responsibilities of the CRO shall include:

- Facilitate the governance of risk management processes throughout the Company.
- Set directions for risk management activities within the Company and facilitate and advise on the execution of risk management plan and related activities across the Company.
- Support management in determining risk appetites, identifying trends, and emerging risks; assist in identifying and assessing risks for new business initiatives, and in evaluating strategic alternatives.
- Consolidate the enterprise Risk Register from each Business Unit/ Enabling Function Heads along with their respective response plans for reporting to the Management Steering Committee. All principal risks

shall be first addressed at the Business Unit/Enabling Function Heads and then reported to the Management Steering Committee.

- The CRO shall assist the management in establishing an effective monitoring system and monitor key enterprise risk(s) on an ongoing basis covering the review of cost, adequacy and effectiveness of risk response plans, completeness and accuracy of risk reporting and timely remediation of deficiencies.
- Assess and evaluate risks associated with proposed capital investments prior to approval of investment decisions.
- Assist in developing and monitoring of Key Risk Indicators (KRIs) to determine the changes in the risk profile and proactively implement risk response measures.
- The CRO shall approve risks proposed by Risk Officers, propose new risks if required, review response plans and monitor KRI threshold breaches.
- Assist in aligning the Risk Management Framework with the Internal Control Framework to ensure key operational risk are adequately and appropriately managed.
- Update Management Steering Committee, Audit and Risk Management Committee on key initiatives taken around risk management, and existing and emerging risks.
- Convene the quarterly Management Steering Committee meetings, participate in the evaluation and decision-making process of the Management Steering Committee for managing key residual risk(s) and track the action items. The CRO shall circulate the agenda, minute the meetings, and circulate the minutes to all participants of the quarterly Management Steering Committee risk review meetings.
- Oversee flow of information and escalation of key residual risk(s) and concerns between the Audit and Risk Management Committee and Management Steering Committee.
- Ensure that a risk management culture is fostered, developed, and embedded within the Company's daily operations over time. Identify training programs for staff with specific risk management responsibilities to enhance awareness.
- Enable the implementation of the ERM Framework and concepts by providing guidance and support to the Risk Managers, as needed.
- Conduct periodic risk management audits and carry out any other activities as may be delegated by the Audit and Risk Management Committee.

C. Risk Ownership

Discussions around risk management and risk related reviews shall be undertaken during the monthly department/ functional level meetings, and risk management shall accordingly form a part of the agenda of such meetings. The departments/ functions/ projects shall deliberate on key residual risks & emerging risks on a monthly basis and on moderate and low risks on a quarterly basis) with their respective HoDs.

7.3.1 Business Unit/Plant and Enabling Function Heads

The roles and responsibilities of the Business Unit/Plant and Enabling Function Heads include:

- They Executive Directors shall set the direction for risk management within their respective units/functions and shall be fulfilling the risk management responsibilities for their respective units/enabling functions.
- The Executive Directors shall approve the proposed risks for the units/enabling functions before being sent to the Central Risk Team.
- Consolidate and present key risks and associated response plans of their respective units/enabling functions to the CRO.

- Ensure adequate justification is given to the CRO on the changes in risk ratings, vis-a-vis the internal and external factors that have played a role in the change in risk ratings, adequacy of existing controls/risk response plans implemented or reasons for not addressing the emerging risk(s) in previous review cycles.

7.3.2 Risk Co-Ordinator

Risk Co-Ordinator will be responsible to coordinate with Risk Officers on the risk management related activities for their respective function. They help in consolidating the risk register. The roles and responsibilities of the Risk Managers include;

- Assist in keeping risk register/risk profile and related response plans updated
- Support in quantification of risks
- Report risks and progress on response plans of the plant/function to the Plant Head/ Functional head.
- Notify the Plant/Enabling Function Heads about significant changes in risk ratings resulting from the risk refresh exercise during the next review cycle.
- Convene plant level meetings, if required

7.3.3 Risk Officers

The final ownership of enterprise risks and risk response rests with the Risk Officers. The Risk Officer is usually a senior member of the function, the head of the department or so, who can drive and monitor the progress of the response plans. The Risk Officers may further delegate the response plans and action plans down the hierarchy to ensure ground-level implementation of response plans.

The roles and responsibilities of the Risk Officers include:

- Identify and assess new and emerging risks within the department.
- Complete Risk Profiles and submit them to Plant/Enabling Functions Heads for approval of proposed response plans.
- Escalate challenges, concerns, or unexpected developments related to existing or emerging risks to the Risk Coordinator.
- Provide sufficient justification to the Plant/ Enabling Function Heads regarding changes in risk ratings, including internal and external factors influencing them.
- Develop a comprehensive risk response plan considering existing controls, proposed measures, and organizational priorities.
- Determine the resource requirements for risk response and seek approval from the Plant/Enabling Function Heads.
- Conduct quarterly reviews of the progress of response plans, ensure implementation and report the status of implementation to the relevant stakeholders.

8. ERM Process and Framework Overview

To effectively manage uncertainty, respond to risks and exploit opportunities as they arise, the Company shall implement an ERM Framework based on leading risk management standards such as COSO 2017 ERM Framework and ISO 31000:2018 Risk Management Framework, that shall lay down the risk management process, in the following steps-

- **Scope, Context and Criteria**: To manage risk management process effectively, it is important to define the scope of the risk management process and understand the internal and external context within NALCO's risk appetite.

- **Risk Assessment**: As a part of comprehensive risk management, the Company needs to identify and assess risks that may affect its ability to achieve its strategy, and business objectives. Risk Assessment is the overall process that includes *risk identification, risk analysis and risk evaluation*.

  a) **Risk Identification***:* The aim of this step is to generate a comprehensive list of risks based on events that may help *(in the case of opportunities)* or impact the achievement of business objectives. Risk identification may be undertaken through workshops and discussions among other activities.

  b) **Risk Analysis:** Risk Analysis involves identification of sources of risk, areas of impact events *(including emerging trends)* and their causes, and potential consequences on the achievement of business objectives. The purpose of risk analysis is to comprehend the nature of risk and its characteristics including contributing factors, impact, likelihood, velocity, controls and their effectiveness

  c) **Risk Evaluation and Prioritization:** Risk evaluation involves comparing the results of the risk analysis *(impact, likelihood, velocity)* with the established risk criteria to determine where additional action is required considering effectiveness of existing controls. This would enable prioritization of risks, basis criticality, and help decide on the appropriate risk management strategy. Prioritization involves ranking the risks based on associated residual risk rating to identify key residual risks.

- **Risk Response:** Risk response refers to response plans developed towards reducing the probability of occurrence or the impact of risk event. Once the company has developed an understanding of its risk profile, it needs to determine if response plans are required, especially in case of key residual risks.

- **Monitoring and Review:** Monitoring and Review involves having definite review forums and defining frequency for monitoring the status of risks to track them periodically. An important aspect of risk monitoring involves identifying and monitoring indicators or signals to sense occurrence of risk, known as “Key Risk Indicators” (*KRIs*). Frequency of reviews is defined to ensure that key residual risks at the Company level are reviewed, together with review of progress of response plans.

- **Recording and Reporting:** The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Reporting ensures that relevant risk information is available across all levels of the Company in a timely manner to provide the necessary basis for risk-informed decision-making. Annual updates are provided to the Board on status of key residual risks and associated response plans.

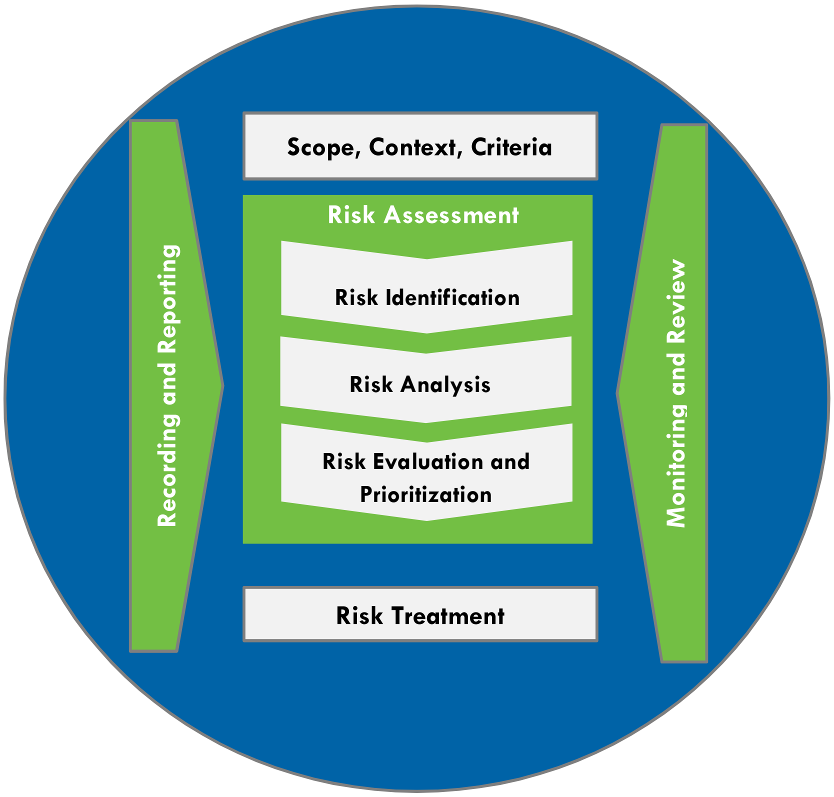

Figure 4: ERM Process

The ERM process includes actions that the Company takes to sense, evaluate, monitor, and respond to internal risks, external risks, and internal and external risks. The detailed guidance to risk management process can be found in the ERM Framework.

9. Communication

This Policy shall be communicated to all Business Units, key corporate functions, projects, and stakeholders involved in the risk management process of the Company.

10. Review

This Policy shall be reviewed at least once in every two years to ensure that it is aligned with the changes in business environment and regulatory requirements related to risk management and reporting. Any changes to the Policy shall be approved by the Board of Directors.

11. Compliance requirements and disclosures

Companies Act 2013, mentions specific requirements that a company needs to comply with regard to risk management that includes the development and implementation of risk management policy, framework, governance structure and systems. In addition, the board and audit committee have been vested with specific responsibilities in assessing the robustness of risk management policy, process and systems.

SEBI LODR 2015 or SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, are rules defined by the market regular i.e., Securities Exchange Board of India or SEBI for transparency and fair disclosure by entities listed in the Indian stock exchanges. The regulation prescribes the requirement for setting up a Risk Management Committee and defines the roles and responsibilities of the Committee around risk management.

COSO 2017 ERM Framework: Is one of the widely accepted risk management standards that focuses on integrating risks with strategic objectives. It also lays emphasis on risk culture and defining risk appetites. The framework includes five components i.e., Governance and Culture, Strategy and Objective Setting, Performance, Review and Revision, Information Communication and Reporting. These components cover 20 principles that provide management and the board with a reasonable expectation that the organisation understands and strives to manage the risks associated with its strategy and business objectives.

ISO 31000:2018 Risk Management Framework: is a leading standard on risk management that focuses on value creation and protection. The standard consists of three main components i.e., Principles, Framework and Process that act as guidelines to establish a risk management framework. ISO 31000 provides direction on how to integrate risk-based decision making and is an open principles-based system enabling organisations to apply the principles in the standard to the organisational context.

12. Disclaimer

In any circumstances, where the terms of this Policy differs from any existing or newly enacted law, rule, regulation or standard governing the Company, the newly enacted law, rule, regulation or standard shall take precedence over this Policy until such time the Policy is changed to conform to the law, rule, regulation or standard.

****

Appendix A – Definitions of Common Terms

Terms	Definitions
Enterprise Risk Management	Enterprise Risk Management involved capability that involves identifying, assessing, measuring, monitoring, and responding to risks across the enterprise in a way that is aligned with the enterprise's objectives and risk appetite
Risk	Risk is defined as "the effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected. Risk is measured in terms of impact, likelihood and velocity.
Uncertainty	Inability to know in advance the exact likelihood or impact of future events.
Challenges/Issue	If the event is certain to happen or has happened the event would be classified as an "issue/challenge". Mostly these challenges/issues are already addressed as part of annual planning processes. A "challenge" is a form of an obstacle that needs to be overcome to achieve desired business outcome. These are "certain" or "on-going" events and hence not classified as risks
Business drivers	Business drivers are the factors/conditions that are vital for the continued success and growth of a business. For different sets of business, the drivers would vary across the organizational value chain depending on its inputs, output and process parameters.
Business Objectives	Objectives are the goals or targets that the organization desires to achieve within a pre-determined timeframe against each business driver.
Risk Appetite	Risk appetite is defined as the amount of risk the organization is willing to take in pursuit of its organizational values. This is the amount of risk the organization is willing to accept/digest and forms its risk appetite.
Risk Category	The broad categories to group risks together form the risk categories. More specifically risks are grouped based on the primary cause of the risk.
Risk Register	Compendium of all risks finalized and detailed with risk definition, KRI, risk response, risk officers
Risk Impact	Result or effect of an event. That may bring a range of possible impacts associated with the event
Risk Likelihood	The assessment of the probability the risk will occur.
Risk Velocity	It is the time that passes between the occurrence of an event and the point at which the organization first feels its effects.
Risk Score	The combined product of risk likelihood and risk impact
Risk Response	A process of assigning risk owners and corporate risk champion for each risk and response; determining the strategy for responding to risks, developing and implementing risk response plans
Response and Contingency plans	Strategies aimed at preventing the occurrence of risk event are called response plans whereas Plan B for risks in case of exigency conditions after the risk play is termed as contingency plans
Root cause analysis (RCA)	Analysis techniques for identification of plausible causes that may lead to the risk event
Key Risk Indicators	"Key Risk Indicators" are rule based quantitative or qualitative triggers from multiple sources of information for early identification of potentially harmful scenarios
Residual Risk	The risk remaining after management has taken action to reduce the impact and/or Likelihood of a risk.
Business Continuity	Any event that has a high impact and high velocity can be terms as business continuity events