# ENTERPRISE RISK MANAGEMENT FRAMEWORK

## Version Control

| | |
|---|---|
| Version No.: 1 | Status: Final |
| Reviewed By: Pratul Kumar Saikia, Chief Risk Officer (CRO) | Date of Review:12-01-2021 |
| Approved By: | Date of Approval: |

## Revision Record Sheet

| S.No. | Revision No. | Date | Description of changes |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Document Custodian:** Chief Risk Officer
**Document Owner:** Director (Finance)

# Contents

# 1. Introduction

Numaligarh Refinery Limited (hereafter referred to as "NRL" or "The Company") is an Assam based public sector undertaking operating in oil & gas sector. It is under the administrative control of Ministry of Petroleum & Natural Gas, Government of India. The company's core business is in the midstream segment in refining operations and undertakes marketing of petroleum products. The company has been classified as a "Miniratna" Public Sector Unit and commenced commercial production in October 2000 (source: NRL website).

NRL has established a process for identification and assessment of risks and mitigation planning, strengthening of internal controls and legal compliance mechanism. Enterprise Risk Management at NRL is governed by a Risk Management Policy which was duly approved by Board of Directors in the meeting held on 26th July, 2012.

Considering the dynamic business environment within which it operates, NRL has identified the need for an efficient, effective and demonstrable Enterprise Risk Management ('ERM') process. It will help support the vision of the organisation.

ERM is a systematic approach to provide reasonable assurance to the Board and the stakeholders on risks associated with the organization; including the risk response strategies adopted by the organization in pursuit of organization's objectives.

All types of organizations face the internal and external factors which influence their operations and develop uncertainty about achievement of organizational strategic objectives. According to ISO 31000, risk is the "*effect of uncertainty on objectives*" and an effect is a positive or negative deviation from what is expected.

The ERM framework document ("ERM Framework") describes the structure, processes, and procedures by which the company will implement ERM across all its business activities.

An effective ERM framework would assist management to maximize value to its stakeholders by maintaining an optimal balance between risks and associated benefits. Additionally, a robust ERM framework would provide proactive management of uncertainties, establish a reliable basis for decision making, optimize allocation of scarce resources, ensure compliance with the laws and regulations, and improve likelihood of achieving strategic objectives of the company.

# 2. Background

## 2.1 Scope

The document details the process for risk management, including process to provide visibility, oversight, control and discipline to drive and thereon improve the organisation's risk management capabilities in a changing business environment.

## 2.2 Purpose

The purpose of this document is to provide the guidelines to establish a comprehensive, aligned, proportionate, embedded and dynamic ERM Framework within the company for effective risk management.

The key benefits of the ERM Framework include, but are not limited to:

- Providing a reasonable assurance to the senior management regarding management of risks;
- Achieving compliance with the laws and regulations;
- Establishing a reliable basis for decision making and planning;
- Improving stakeholder's confidence and trust in the organization;
- Allocating and utilize resources effectively for risk responses; and
- Achieving efficiency, effectiveness, and efficacy in the operations, projects, and strategy.

The fundamental objective of the ERM is to ensure that the risks are identified and managed in a prioritized, consistent, effective and efficient manner at all levels within the company

To realize the ERM objectives, The Company aims to ensure that:

- Risks are identified, assessed and treated by the organization in a timely manner;
- The risks are reported and/or escalated to the senior management to initiate necessary risk response plans;
- The potential impact of identified risks on the organization is continuously monitored and controlled within the risk appetite of the organization; and
- Risk management activities are not considered in isolation; but rather, they are embedded within the standard business processes, operations, and management decision making process.

## 2.3 Applicability

The framework is applicable across all activities performed by Numaligarh Refinery Limited from the date it is approved by the Risk Management Committee (RMC).

## 2.4 Administration

Any revision to the framework will be incorporated after endorsement by the ERM Steering Committee followed by the approval of the RMC. Any introduction of new unit to manage Enterpriser Risk Management activities will be made following the approval by the Chief Risk Officer (CRO).

## 2.5 Elements of ERM Framework

ERM Framework constitutes of three elements namely Risk Management Policy, Risk Management Charter and Risk Process Manual, which are to be read in totality. The ERM Framework lists down the details about enterprise risk management process to be followed during risk identification, assessment, response, review and reporting. It also describes the risk governance structure and the respective roles and responsibilities of constituent committees and risk practitioners within the organization.

# 3. Risk Management Policy

Risk Management Policy established by NRL describes how the ERM framework shall be implemented consistently throughout the organization. The Policy serves as a holistic set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving enterprise risk management throughout the organization.

## 3.1 Objectives

The objective of the Policy is to establish a structured approach to enterprise risk management for NRL that is integrated with the organization's strategic and business planning processes. This Policy document highlights the management's intent to align strategy, processes, people, culture, technology and governance with the purpose of evaluating and managing the uncertainties faced by the organization while creating value. Further, it sets out management's intent and commitment towards implementing a structured, comprehensive, dynamic, integrated, and robust ERM framework.

## 3.2 Policy Principles

NRL is committed to adopt a proactive approach to enterprise risk management which is based on the following underlying principles:

- The company endeavours to ensure risk aware culture across the organization;
- The company strives to anticipate and take preventive action to respond to risks within its risk appetite;
- The company aligns & integrates varying views on enterprise risk management and reviews & monitors a uniform ERM Framework across the organization;
- The company strengthens the governance framework by focusing on proactive risk-informed decision making within the organization;
- Establish linkage between the organization's vision, mission, strategic objectives and the ERM strategy; thus, ensure that ERM supports NRL's efforts to achieve its objectives;
- All employees of the company take responsibility for the effective management of risks in all aspects of the business;
- Provide the best available information in identifying and analysing risks associated with NRL;
- Provide resources and authority to the ERM Function to ensure effective management of the ERM framework; *and*
- Strive continually to enhance ERM framework to ensure its alignment with the latest established standards as well as leading industrial practices.

## 3.3 Design of Risk Management Policy

### 3.3.1 Mandate & Commitment

Management shall demonstrate strong and sustained commitment in order to establish a robust ERM framework within the organization. The management shall:

- Define and endorse the Risk Management Policy;
- Communicate its approach and commitment towards the ERM initiatives; and
- Ensure that the culture and strategy of the organization is aligned with the established Risk Management Policy.
- Support transparent reporting of risks related information without the fear of retaliation amongst the employees.

### 3.3.2 Alignment with Industry Standards

Management shall ensure that the framework is aligned with the leading international standards and industry practices. Framework shall be reviewed periodically to ensure changes/revisions within the respective standards and practices are incorporated.

### 3.3.3 Assign Accountability

Management shall ensure that there is clear accountability, authority and appropriate competence for managing risks, including that for implementing and maintaining the ERM processes. This can be facilitated by:

- Establishing clear roles and responsibilities for the individuals within the organization who are in the best position to manage risks, including associated controls and response plans;
- Establishing the framework to monitor progress of management action plans and its impact of the risk; and
- Assigning appropriate level of recognition and rewards.

### 3.3.4 Integrate with the organizational processes

Management shall ensure that ERM principles are embedded across all policy, procedures and processes established within the organization. Any new initiative, process, and/or change management that is undertaken within the organization shall be aligned with ERM principles.

### 3.3.5 Establish (internal/external) communication and transparent reporting mechanism

The ERM Function shall establish a clear internal communication protocol in order to develop a structured risk reporting mechanism. Transparency in risk reporting is to be ensured to enable proactive reporting of the risks by risk practitioners and staff within the organization.

Risk escalation protocols shall be defined within the automated risk management process to facilitate timely review and monitoring by management especially with regards to critical/severe risks.

Additionally, an external communication framework shall be established to communicate and report risks with regards to the external stakeholders such as contractors and suppliers, as required.

Necessary controls shall be established to protect sensitive / confidential information about the organization and its operations while communicating risk information within and/or outside the organization.

Organization shall ensure that no employee shall face retaliation for sharing risk related information through a right channel in the interest of the organization.

### 3.3.6 Training and Awareness

Adequate training and awareness initiatives shall be taken to communicate benefits of the ERM framework to all stakeholders and establish risk aware culture within the organization.

## 3.4 Regulatory Framework

**As per Section 134 (3) (n) of Companies Act 2013:**

*"Director's report in annual report of the Company shall include 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"*

**As per Schedule IV (Code for Independent Directors) read with Section 149(8) of Companies Act 2013 detailing therein that the Independent Directors shall;**

(1) *"Help in bringing an independent judgement to bear on the Board's deliberation especially on issues of strategy, performance, **risk management**, resources, key appointments and standards of conduct" and*

(2) *"Satisfy themselves on the integrity of financial information and that financial controls and the systems of **risk management** are robust and defensible"*

(Space left blank intentionally)

# 4. Risk Management Charter

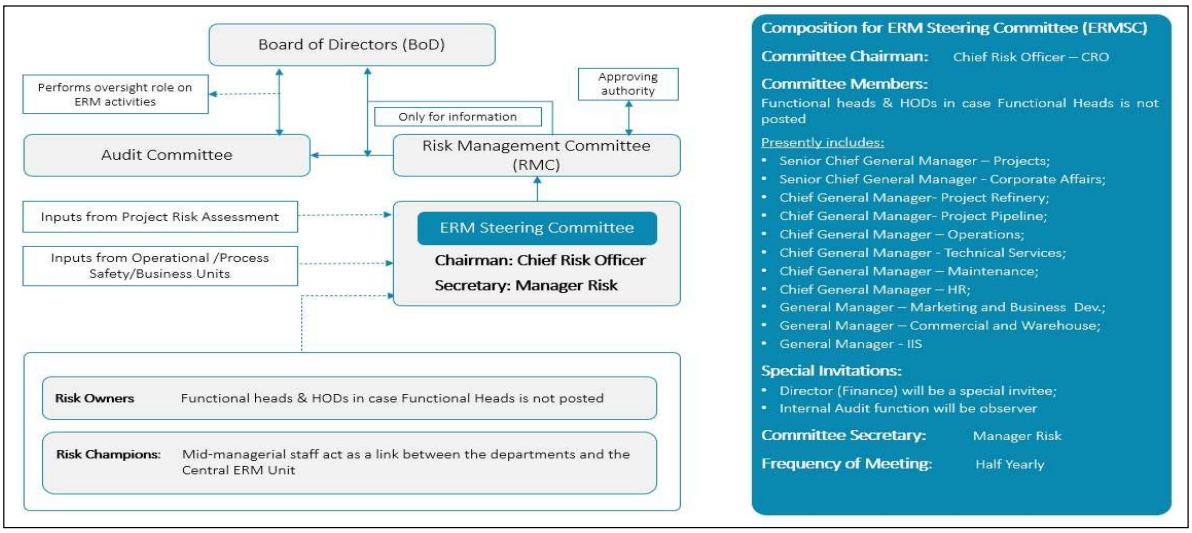



Fig 1: NRL Enterprise Risk Management Governance Structure

Risk Management Charter comprises of Risk Governance Structure including RACI matrix that are defined to ensure clarity in terms of roles and responsibilities of individual stakeholders involved in risk management process. (*For detailed roles & responsibilities and RACI Matrix refer to* Annexure 7.1 *and* Annexure 7.2 *respectively)*

The Risk Management Charter aims to;

- Provide a sound basis for integrated enterprise-wide risk management as a component of good corporate governance; *and*
- Define the risk governance structure to establish and thereby promote strong tone at the top to build risk culture within the organization;

The governance framework to direct, manage, and report risk management activities across the Company in accordance with ERM framework is as described below:

## 4.1 Board of Directors (BoD)

The BoD is responsible for performing oversight on the ERM activities of the company. It is informed of approved risk management framework/risk assessment criteria/risk register for the organization.

## 4.2 Audit Committee (AC)

The Audit Committee is constituted in accordance with provisions of section 177 of Companies Act 2013. The Audit Committee shall be responsible for evaluation of risk management systems of the company.

While the BoD ensures oversight over the overall establishment of the ERM framework; the AC may provide its independent assurance to the BoD regarding the effectiveness and adequacy of the risk management practices.

The Internal Audit function may provide independent assurance on the risk management activities conducted across the organization in accordance with its mandate and the responsibilities assigned by the Audit Committee.

## 4.3 Risk Management Committee (RMC)

The Risk Management Committee is the nodal committee to oversee the risk management activities across the organization. The RMC is accountable to the Board on the delivery of risk management activities in accordance with the ERM Framework comprising of the Charter, Policy and Risk Process Manual. Key activity of RMC is to approve risk registers & respective response plans.

The Risk Management Committee comprises of the Director (Technical), Director (Finance) and Independent Directors. The committee meets annually to deliberate upon risk management activities within the organization.

## 4.4 ERM Steering Committee (ERMSC)

The members of the ERMSC and ERMSC Secretary are nominated by the Risk Management Committee (RMC) in consultation with CRO. The committee is comprised of members from the Senior Management (Functional/Departmental Heads) of the company.

The ERMSC oversees and guides management in developing and maintaining the risk management framework for the organization. It advises departments/functions on risk management activities & reviews respective risk registers and response plans for presentation before & approval by RMC. ERMSC shall report risks; including the status of risk response plans to the RMC on a yearly basis.

**Composition of ERM Steering Committee (ERMSC)**

Chairman: Chief Risk Officer

The members of the ERMSC consists of Functional heads & HODs in case Functional Heads is not posted. Presently it includes following members;

- Senior Chief General Manager (Projects)
- Senior Chief General Manager (Corporate Affairs)
- Chief General Manager (Project Refinery)
- Chief General Manager (Project Pipeline)
- Chief General Manager (Operations)
- Chief General Manager (Technical Services)
- Chief General Manager (Maintenance)
- Chief General Manager (HR)
- General Manager (Marketing & Business Development)
- General Manager (Commercial & Warehouse)
- General Manager (IIS)

Secretary: Manager- Risk

Special Invitees: Director (Finance)

Observer: Internal Audit Head

**Operating Guidelines:**

- ERMSC meetings are held on a half yearly basis at a minimum.
- If the members, are unable to attend the meeting, they are represented by their acting employees (alternate members) from the organization;
- For voting purposes, each member has one vote and resolutions are passed if approved by a majority vote. In case of an equality of votes on any matter, the Chairman provides the casting vote. Alternate members have voting right only if the corresponding members are absent;

- The quorum for conducting ERMSC shall be minimum 50%.; (Refer Annexure 7.1 on detailed roles and responsibilities of ERMSC)
- Due to change in organizational structure, there may be instances of creation of new departments/positions. In such scenario, CRO shall have right to appoint the designated Heads of such departments, as the member of ERMSC during the course of year. Any revisions in the composition of ERMSC shall be informed to RMC in the next meeting.

**Operating of the Committee**

- The main duties and responsibilities of the Secretary shall be to:
    - Co-ordinate and make arrangements to conduct the Committee meetings;
    - Provide notice for each meeting to the Committee Chairman, members, and any other participant, together with agenda of items to be discussed and other documents, as appropriate;
    - After each meeting, prepare draft Minutes and resolutions and distribute it for review. Subsequently, circulate the finalized versions of the Minutes and resolutions to each Committee member and other recipients, as appropriate; *and*
    - Retain records of all Minutes, resolutions, Committee reports, and records of proceedings ensuring confidentiality of all Committee proceedings.

The Committee will make regular reports to the RMC and Board/AC. The Committee will review and reassess the adequacy of this charter, in a timely manner and recommend any proposed changes to the RMC for its consideration.

**Meeting notice**

At least one (1) week prior to the meeting, the Committee Secretary shall issue Agenda for the meeting to Committee Chairman, members, and any other individual who is required to attend the meeting.

If Committee Members are unable to attend the meeting, they shall nominate an alternate individual to represent them during the meeting. The Committee member shall be accountable for the actions / decisions taken by the nominated individual during the meeting.

## 4.5 Chief Risk Officer (CRO)

As the Chairperson of the ERMSC, the Chief Risk Officer is responsible for overseeing the functioning of the ERM Steering Committee.

The CRO liaises with the RMC and ERMSC to ensure coordinated flow of information for decision making. The CRO is also responsible for establishing the ERM framework and oversees the preparation of the Risk Management Report.

## 4.6 ERMSC Secretary

The Manager- Risk serves as the secretary of the ERM Steering Committee. He/she is responsible to ensure meetings of ERMSC are conducted as scheduled and ensure documentation in relation to notices, minutes and resolutions of meetings are maintained.

## 4.7 Risk Owners

Risk Owners are individuals within the organization who are assigned responsibility to identify, review, monitor risks and contribute towards risk response plans for their respective department and enterprise level risks, wherever applicable. Risk Owners consist of senior management and the heads of business units/departments/functions (Sr. CGM, CGM and GM). Risk Owners are deemed accountable and responsible for management of risks within their concerned departments/functions.

The Risk Owners put in coordinated efforts to identify & discuss the risks in detail, identify gaps in risk and controls, propose risk response plans and review the implementation status of response plans.

### 4.8 Risk Champions

Risk Champions are appointed by the risk owners to support in identifying risks and response plans for respective departments/functions. Risk Champions support Risk Owners to assess, review, monitor and react to risks, evaluate and validate the status of risks and propose controls/response plans.

Risk Champions are responsible for risks at the operational level. The mid-managerial staff will be assigned the responsibility of Risk Champion. The Risk Champion function as a link between the business unit and the Central ERM Unit.

Risk Champions help to implement risk management elements in key business processes and procedures within the company. An active network of Risk Champions serves as an effective way to develop a strong risk management culture.

## 5. Risk Process Manual

### 5.1. Risk Appetite and Tolerance

Prior to assessing and evaluating the identified risks, it is imperative to understand the concepts of Risk Appetite and Risk Tolerance that help in objectively formulating adequate risk response plans of the organization. The concepts of Risk Appetite and Tolerance Limits are as stated below;

Establish Risk Appetite and Tolerance Limits:

**Risk Appetite** is defined as the type and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. The senior management shall thoughtfully define the risk appetite of the organization to ensure that sufficient value has been assigned towards uncertainties.

Risk Appetite provides insights on the nature and extent of risk acceptable to the company with regards to salient aspects namely projects, services, safety and compliance in pursuit of value/achievement of objectives. With the approval of the RMC, the management shall revisit and reinforce risk appetite over time in consideration of new and emerging developments and to ensure risks are managed within acceptable variation.

An organization may articulate detailed risk appetite statements in the context of;

- Strategy and business objectives that align with mission, vision and core values; and
- Performance targets of the organization

An organization may define its risk appetite depending on its propensity to take risks which is as diagrammatically explained below;

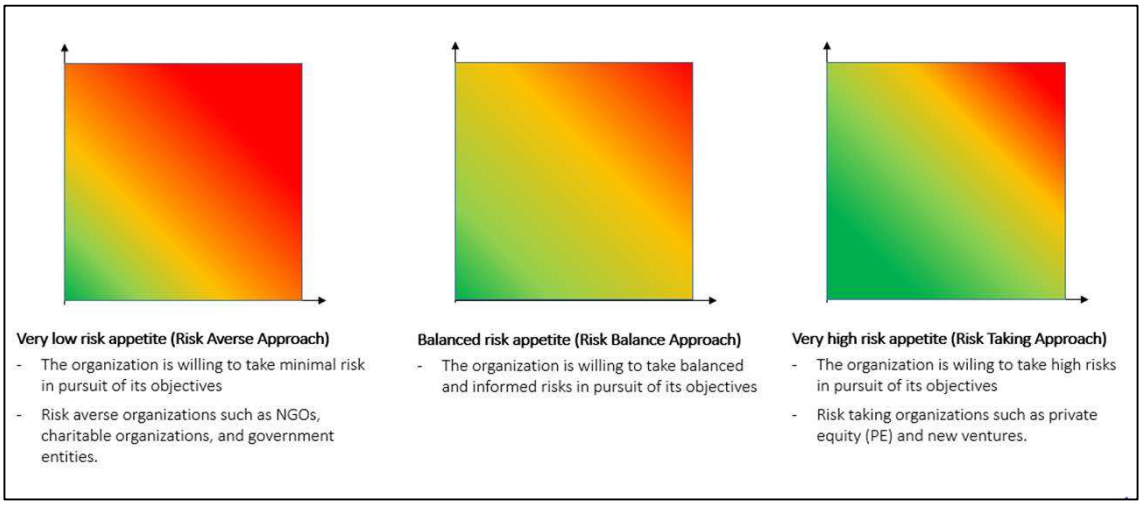



Fig 2: Different risk taking approaches adopted by organizations

**Risk Tolerance** is the maximum amount of risk associated with each risk-taking activity that the company is willing to accept in pursuit of its mission, vision and strategic objectives and also represents the thresholds beyond which the company is not willing to accept risk.

The risk appetite and tolerance limits shall be determined by RMC and subsequently disseminated throughout the organization.

When considering tolerance limits, it is vital to gauge risk acceptability levels by testing these limits with management.

Tolerance limits shall be set based on company's propensity to absorb risk. The risk tolerance levels of the organization are depicted through five (5)-pointer impact scale adapted by the organization to assess risks. (As given in Annexure 7.5). The tolerance limits shall be modified based on experience and maturity levels of risk management.

## 5.2 Risk Management Process

An effective management framework becomes the foundation of a successful Enterprise Risk Management (ERM) exercise, as it embeds risk management as an integral part of the decision making process. The ERM framework assists management to achieve its strategic objectives by maintaining optimal balance between risks and associated benefits.

The ERM framework of the organization shall be based on the following principles:

| | |
|---|---|
| **Proportionate** | ERM activities shall be proportionate to the level of risk faced by the organization |
| **Aligned** | ERM activities shall be aligned with the activities in the organization |
| **Comprehensive** | ERM approach shall be comprehensive, in order to ensure a proactive exercise |
| **Embedded** | ERM activities shall be embedded within the organization |
| **Dynamic** | ERM activities shall be dynamic and responsive to emerging and changing risks |

In order to manage risks in a systematic manner, the Risk Management Process includes the following steps:

A. Define Scope, Context and Criteria;

B. Risk Assessment comprising of the following activities;

i. Risk Identification;

ii. Risk Analysis;

iii. Risk Evaluation and Prioritisation;

C. Risk Treatment;

D. Monitoring & Review;

E. Communication and Consultation;

F. Recording and Reporting

## A. Define Scope, Context and Criteria

The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process and understanding the external & internal context.

### (i). Defining the Scope

The organization shall define the scope of its risk management activities. As the risk management process may be applied at different levels (e.g. strategic, operational, project or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organizational objectives.

When planning the approach, considerations include:

- Objectives and decisions that need to be made;
- Outcomes expected from the steps to be taken in the process;
- Time, location, specific inclusions and exclusions;
- Appropriate risk assessment tools and techniques;
- Resources required, responsibilities and records to be kept; *and*
- Relationships with other projects, processes and activities.

### (ii). Establishing the external and internal context

The external and internal context is the environment in which the organization seeks to define and achieve its objectives.

The context of risk management process shall be established from the understanding of the external and internal environment in which the organization operates and shall reflect the specific environment of the activity to which the risk management process is to be applied. These conditions could pose risks or present opportunities that could impact the company's day to day operations or the achievement of the company's objectives.

The evaluation of the external context includes, but is not limited to:

- Analysis of local, national, regional, and international trends / industry scenarios;
- External stakeholder's relationships, perceptions, values, needs and expectations;
- Analysis of political, economic, social, technological, extended enterprise and legal (PESTEL) factors; and
- Relationships, perceptions and values of stakeholders.

The evaluation of the internal context includes, but is not limited to:

- Review of vision, mission and values of the organization;
- Review of governance framework, organization structure, roles and responsibilities;
- Review of effectiveness and adequacy of policy, procedures, processes including key business strategies, objectives and tactics;
- Review of changes in ownership i.e. investment / divestment by the shareholders;
- Review of initiation and/or termination of major initiatives e.g. refinery expansion, new product development, etc.
- Review of changes in the capital structure of the organisation;
- Review of award / termination of major contractual commitments / stakeholders;
- Review of interfaces with the external entities such as clients, consultants and contractors;
- Review of performance monitoring framework;
- Review of information systems and communication channels; *and*
- Strength, Weakness, Opportunities and Threat (SWOT) analysis.

### (iii). Defining Risk Criteria

The organization shall specify the amount and type of risk that it may or may not take, relative to objectives. It shall also define the criteria to evaluate the significance of risk and to support decision making processes. Defining risk criteria involves deciding;

- The nature and types of consequences to be included and how they will be measured;
- The way in which probabilities are to be expressed;
- How a level of risk will be determined;
- The criteria by which it shall be decided when a risk needs treatment;
- The criteria for deciding when a risk is acceptable and/or tolerable;
- Whether and how combinations of risks shall be taken into account.

The risk criteria is determined on the basis of the impact and likelihood criteria defined as given in Annexure 7.5

While risk criteria shall be established at the beginning of the risk assessment process, they are dynamic and shall be continually reviewed and amended, if necessary.

## B. Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment shall be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It shall use the best available information, supplemented by further enquiry as necessary. Risk assessment provides an understanding of risks, their causes, consequences and their probabilities.

The risk assessment process provides input to decisions about:

- Whether an activity shall be undertaken;
- How to maximize opportunities;
- Whether risks need to be treated;
- Choosing between options with different risks;

- Prioritizing risk treatment options; *and*
- The most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

### (i). Risk Identification

Risk identification process is to determine the risks that could interrupt operations, affect the reasonable expectation of achieving the strategy and business objectives. This phase includes performing detailed analysis of business operations to identify uncertainties associated with the department/function. Risk Identification includes the following action steps:

a. Identification of risks is the responsibility of each department/function and performed based on the below methods:

- **Risk Workshop:** Conduct set of interviews / risk workshops with the key management personnel to assess their perception about the key risks associated with the organization;
- **Industry and market research:** Study the current market trends, industries in the same domain and prepare a list of probable risks for the organization;
- **Scanning of Internal and External Environment**: Analysing internal and external environment relevant to the company and industry, in order to identify potential risks to the business through SWOT and PESTEL Analysis (As in Step 5.2 (A)(ii));
- **Inputs from Annual Business Plan (ABP) & Long term strategy**: Study and assess the challenges and assumptions made in the ABP and Long term strategy. Additionally, review of documented information such as financial statements, performance scorecards, project reports, etc. can be used to gather insights about the organization;
- **Leadership Inputs:** Senior Management to guide the corporate/department/ functions in identifying the top risks which may impact the company performance;

After the risks have been identified, they will be documented within risk register that will include the following aspects (Refer to Annexure 7.3 for Risk Register Template):

- **Risk statement:** Articulation of risk statement may include brief description of event and a major impact of the risk;
- **Risk Category**: This is associated with the category of the risk which could be Financial, Operational, Reputational, Regulatory, Extended Enterprise, Strategic and Technological (FORREST) (Refer Annexure 7.4);
- **Business Unit**: This includes the respective business unit/department/function to which the identified risk pertains to;
- **Contributing factors:** This would include the various causes that accentuate the occurrence of risks. The contributing factors are broadly categorized into *People* and *Policies;*
- **Risk Owner:** Individual responsible to identify, review, monitor risks and contribute towards risk response plans associated with his/her area of functioning;
- **Risk Champions:** Individual appointed by the risk owners to support in identifying risks and response plans for respective departments/functions;
- **Business Objective**: This would describe the strategic/operational objectives associated with the identified risks. Identification of the objectives ensures proactive steps are taken in response to associated risk and achievement of respective objective.

b. Risk statements are developed and documented in the risk register for further assessment and analysis.
c. Once a risk is identified, the organization shall identify any existing controls such as design features, people, processes and systems
d. Risk Owner and Risk Champion are assigned for all risks identified by the respective department/functions
e. The Risk Owners (supported by Risk Champions) shall be responsible for risk assessment and development of risk response plans within their department/functions.
f. The Chief Risk Officer shall ensure that the risk register is reviewed on a half yearly basis at minimum.

### (ii). Risk Analysis

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine the level of risk.

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Once the risks have been identified, risk assessment can be undertaken which involves analysing and evaluating the probable impact and likelihood of risk occurrence (Refer Annexure 7.5 for risk assessment criteria). In this phase, feedback is elicited regarding rating – i.e. impact and likelihood of identified risks, thereby arriving at the associated risk criticality. This activity includes the following action steps:

a. Assess the ***Impact*** rating of risk on the scale of 1 to 5, depending on the severity of impact of the identified risk.

b. Assess the ***Likelihood*** rating of risk on the scale of 1 to 5. Likelihood is the chance/probability of occurrence of risk

c. During the risk assessment the following inputs shall be considered:

- Prior experiences and instances;
- External information sources;
- Analysis of past and current data;
- Inputs from department/function heads and management (Risk Owners)

d. Compute the ***Risk Criticality Score*** i.e. (Impact) * (Likelihood)

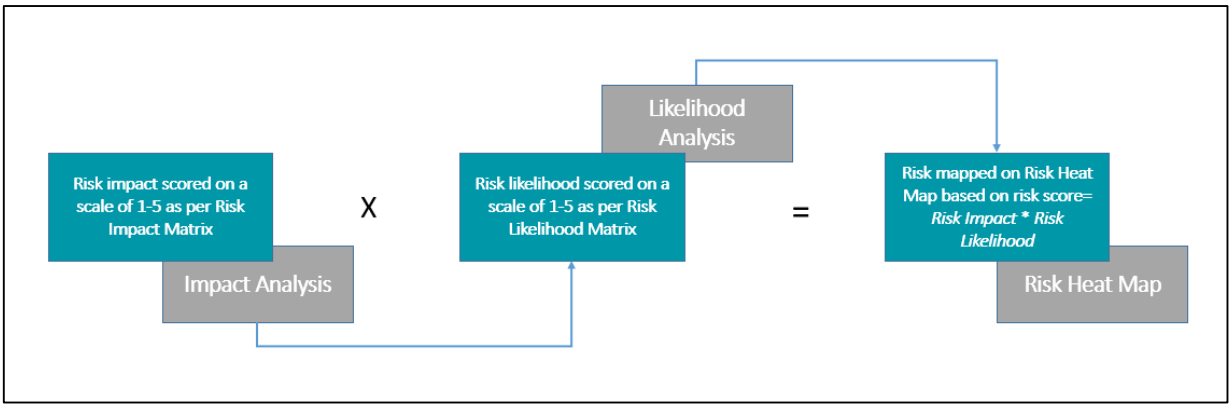



Fig 3: Computation of Risk Score

e. The risk will be classified into ***Severe, Critical, Moderate and Acceptable*** based on the below Risk Rating Criteria (The rating will be auto computed in risk register template).

| Risk Rating | Criteria |
|---|---|
| Severe | Risk score ≥16 and ≤25 |
| Critical | Risk score ≥10 and ≤15 |
| Moderate | Risk score ≥5 and ≤9 |
| Acceptable | Risk score ≤4 |

**Assessment of Controls**

The level of risk will depend on the adequacy and effectiveness of existing controls.

Questions to be addressed include:

- What are the existing controls for a particular risk?
- Are those controls capable of adequately treating the risk so that it is controlled to a level that is tolerable?
- In practice, are the controls operating in the manner intended and can they be demonstrated to be effective when required?

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

### (iii). Risk Evaluation and Prioritisation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to;

- Do nothing further;
- Consider various Risk Treatment Options;
- Priorities for Treatment;
- Undertake further analysis to better understand the risk;
- Maintain existing controls; *and*
- Reconsider Objectives.

The Risk Rating enables prioritization of risks and thereby, presentation of key risks. Based on the above risk rating, the risks are mapped on to a two-dimensional matrix called Risk Heat Map. *(Detailed description of risk prioritization is depicted with Heat Map as given in* Annexure 7.5*)*

Basis of the criticality, organization shall identify acceptable and non-acceptable (severe/critical) risks. The existing controls established shall be considered during risk assessment.

Key risks which are essentially "Severe/Critical" risks shall be identified, assessed and reported to the Board & Audit Committee. Severe risks are those risks which possess the potential to fundamentally undermine the ability of the company to achieve its strategic objectives. **An example of severe risk is as given in** Annexure 7.7

Decisions shall take into account the wider context and the actual and perceived consequences to external and internal stakeholders. The outcome of risk evaluation shall be recorded, communicated and then validated at appropriate levels of the organization.

(Space left blank intentionally)

## C. Risk Treatment

**Risk Treatment or Response** involves identifying the most appropriate strategies to manage the risks and bring them down to an acceptable **risk appetite** level. Risk Treatment/Response shall include the following action steps:

a. Develop response plans for risks targeted towards reducing the probability of occurrence/likelihood or the impact of risk events. The Risk Response plans are classified as follows;

| Risk Response | Description of Plans |
|---|---|
| Treat | **Treat The Risk** by identifying specific response actions that shall be taken to reduce the likelihood and/or impact of the risk.<br>Response Plans shall include a timeline for monitoring and confirming implementation of plans |
| Transfer | **Transfer Responsibility** for the risk to a third party, usually by availing insurance or signing a contract. |
| Tolerate | **Tolerate (Accept) The Risk** if no further response plans can be implemented/required to be implemented and risk is to be monitored on a periodic basis in such a scenario. |
| Terminate | **Do Not Proceed.** Find another way to achieve the required objective.<br>Risks cannot always be avoided or eliminated completely. Prudent decisions are required to eliminate the cause/process which results in this risk |

**Fig 5: Risk Response Plans**

b. Risk response plans for department and enterprise level risks are formulated by Risk owners in consultation/guidance from senior management. The information shall be presented in the subsequent ERMSC meetings;

c. Risk response plans shall not only consider the corresponding risk appetite, tolerance limits of the organization but also consider the timeframes and budget requirements/ resource implications for implementation;

d. Risk response plans shall be time bound and responsibility driven to facilitate future status monitoring and reporting to the senior management and Board to timely address the consequences of such risks in case they materialise;

e. The risk assessed as "key" risk (critical/severe) that are thereby to be reported to Board & Audit Committee, are to be profiled in "Risk Profile Format" as provided in Annexure 7.6. The profile contains details of the risk, its contributing factors, risk scores, controls and response plans;

f. Risk treatments, even if carefully designed and implemented may not produce the expected outcomes and could produce unintended consequences. Monitoring and review needs to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment are effective.

g. Risk response plan for severe/critical/moderate risks shall be provided by Risk owner and will be presented in subsequent ERMSC meeting.

## D. Monitoring and Review

It is critical to institute an effective system of escalation, to ensure that specific issues are promptly communicated and followed up appropriately. Escalation shall enable timely action by appropriate level of management to respond effectively to key risks (critical/severe) faced by the organization.

**The risk escalation process for the identified critical/severe risks is as given below;**

| # | Risk Criticality | Risk Escalation |
|---|---|---|
| 1 | Acceptable | Not Applicable |
| 2 | Moderate | Not Applicable |
| 3 | Critical | • Notification/Alerts shall be provided to the CRO and Director (Finance) on the identified critical risks by the risk owners<br>• Risk Owners shall prepare risk response plan and update the CRO<br>• Further, CRO shall update the ERMSC within 10 days of notification for further deliberation and action on the identified critical risk |
| 4 | Severe | • Notification/Alerts shall be provided to the CRO and Director (Finance) on the identified severe risks by the risk owners<br>• Risk Owners shall prepare risk response plan and update the CRO<br>• Further, CRO shall update the ERMSC within 5 days of notification for further deliberation and action on the identified severe risk |

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes shall be a planned part of the risk management process, with responsibilities clearly defined.

**Risk Reviews** ensure evaluation of risks on predetermined intervals to track the dynamics of the internal and external environment continuously. Ongoing review is essential to ensure that the management plans remain relevant. Factors which may affect the likelihood and impact of an outcome, may change, as may the factors, which affect the suitability or cost of the various response plans.

Risk review includes the following action steps:

a. RMC and ERMSC reviews the implementation status of risk response plans respectively. Review aims at assessing the progress of risk response plans;

b. Risks identified and assessed pertaining to different departments/functions are consolidated and shared with ERMSC and subsequently RMC for review and approval;

c. Risk Register shall be reviewed, assessed and updated on a periodic basis, with identified risks being reassessed based on priority.

Re-assessment and review of the risks shall be performed as per the below frequency:

| Risk Rating | Review Frequency |
|---|---|
| Severe | Half Yearly |
| Critical | Half Yearly |
| Moderate | Annually |
| Acceptable | Annually |

E

ERM Framework comprising of Policy, Charter and Process Manual is subject to systematic reviews, including reviews from independent authorities, to achieve continual improvement to ensure that it is aligned with the changes in business environment and regulatory requirements.The framework shall be reviewed externally within 5 years from the date of approval by the RMC.

As a part of framework review, management shall:

- Benchmark the established practices against the latest standards such as ISO 31000 and/or COSO ERM framework ;
- Review progress of risk management activities against a defined schedule; *and*
- Recommend internal and external/independent reviews of the ERM framework.

The management shall promote continual improvement of the ERM framework. The framework shall be revised based on the results of independent reviews, current state assessment of risk maturity, performance monitoring and lessons learnt during the execution phase. Such revisions and updates to the ERM framework enable itself to achieve a higher level of maturity.

## E. Communication and Consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making.

Communication and consultation with appropriate external and internal stakeholders shall take place within and throughout all steps of the risk management process.

The ERMSC shall ensure that employees of the organization are regularly updated about risk management activities and related initiatives. NRL shall invest in training and development initiatives and awareness sessions within the organization for risk practitioners and staff as a part of continual development.

## F. Recording and Reporting

The risk management process and its outcomes shall be documented and reported through appropriate mechanisms. In this regard, recording and reporting shall aim to:

- Communicate risk management activities and outcomes across the organization;
- Provide information for decision-making;
- Improve risk management activities;
- Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Risk Reporting is an integral part of ERM process and critical from monitoring perspective. Risk Reporting shall include the following action steps:

a. The frequency of reporting shall be commensurate with the severity and priority of the risk. Reporting shall enable management to determine the types and amount of risk assumed by the organization, its ongoing appropriateness, and the effectiveness of existing risk responses;

b. In order to facilitate the Risk Reporting process, risks identified and assessed pertaining to different departments/functions shall be consolidated and accordingly updated within the DRM Tool;

c. The current status of key risks shall be monitored through the risk reporting dashboard. Risk Dashboard shall be presented within ERMSC, RMC and Board meetings for review, inputs and monitoring. Reviews shall be undertaken by ERMSC and RMC on a half yearly and yearly basis at minimum respectively;

d. Comprehensive risk report (risk management report) shall be prepared and submitted to the management (BoD) on a yearly basis that will foster discussions with regards to performance of the organization in meeting its business objectives and impact of potential risks achieving those objectives. Additionally, progress of risk assessment shall be monitored and reported at every phase of implementation.

**The risk reporting process for risks is as given below;**

| # | Risk Criticality | Risk Reporting and Monitoring |
|---|---|---|
| 1 | Acceptable | Not Applicable |
| 2 | Moderate | Not Applicable |
| 3 | Critical | Half Yearly reporting to ERMSC, Annually reporting to the RMC and the Board |
| 4 | Severe | Half Yearly reporting to ERMSC, Annually reporting to the RMC and the Board |

**Timelines for risk management reporting have been summarized below:**

| Activities | Timelines |
|---|---|
| Risk Register to be presented to the ERMSC | Half Yearly |
| Review and approval of risk register by RMC | Annually |
| Risk Reporting to Board by RMC | Annually |

The risks shall be assessed and reviewed half yearly, with the risk register of respective departments/functions presented to ERMSC. Critical and severe risks shall be escalated for reporting and monitoring purposes to the ERMSC on a half yearly basis and to the RMC/Board on an annual basis.

Key risks (severe/critical) thus identified for the organization with the Risk Management Report, shall be reported and presented to the Board of Directors annually.

The Chief Risk Officer along with the Risk Owners shall be responsible for ensuring that the documentation has been developed and maintained up to date.

**The key documents pertaining to the ERM process that shall be maintained by NRL are:**

- ERM Framework comprising of Policy, Charter and Process Manual;
- Consolidated Risk Register and department/function risk registers;
- Agenda and Minutes of meetings of (MoM) of Risk Management Committee and ERM Steering Committee

### 5.3 Technology Dynamism

Organizations shall leverage information systems to help sustain enterprise risk management. Digitization of the risk management helps in unifying different levels of information on documentation, workflow, assessment and analysis, reporting, visualization, and remediation of risks. Automation offers a common platform for data aggregation, maintaining data quality and bringing transparency in risk management activities.

NRL has embarked on ensuring technological integration of its risk management activities through the implementation of Deloitte Risk Monitor (DRM) Tool. The tool enables digitization of risk management practices and provide necessary information to the management to support risk based decision making approach within the organization.

The salient features of DRM Tool are illustrated below;

1. Configure role based accesses to ensure integrity and confidentiality of risk information;
2. Schedule constituent committee meetings, updation of agenda, minutes and action points;
3. Record risks identified with contributing factors and undertake assessment of respective risks through risk workshops;
4. Document, review and monitor the existing controls and response plans for the assessed risks;
5. Facilitate escalation of risks basis their criticality and associated trends;
6. Enable robust risk reporting mechanism across higher levels of management within the organization;
7. Monitor critical risks and associated trends through dynamic risk dashboards.

## 6. Disclaimer

In any circumstances, where the terms of this framework differ from any existing or newly enacted law, rule, regulation or standard governing the company, the newly enacted law, rule, regulation or standard will take precedence over this framework until such time the framework is changed to conform to the law, rule, regulation or standard.

(Space left blank intentionally)

# 7. Annexures

## 7.1 Roles & Responsibilities

The risk management roles and responsibilities for the ERM framework implementation will be as follows:

| Role | Responsibility |
|---|---|
| ERM Steering Committee (ERMSC) | • Embed strong Tone at the Top to promote risk aware culture across all levels within the organisation;<br>• Develop and maintain risk management framework comprising of charter, policy & process manual and ensure that it is aligned with the latest standards as well as leading industry practices;<br>• Advise departments and functions on Risk Management Framework;<br>• Receive inputs from risk assessments undertaken namely: Safety and Occupational Risk Management, Financial Risk Management, and Project Risk Management; accordingly, initiate necessary actions to respond to critical risks associated with organization;<br>• Review and approve the Risk Management Report including selection of critical risks for approval of the RMC and to inform the Board/Audit Committee;<br>• Undertake assessment of risks identified & response plan for the organization;<br>• Ensure updation of consolidated risk register on half yearly basis, with risk profile and respective response plans;<br>• To report periodically (yearly) to the RMC on the critical risks of NRL; including the progress of associated risk response plans;<br>• Monitor the execution of risk management activities and share best practices among risk practitioners of the organization;<br>• Recommend training programs for staff with specific risk management responsibilities to enhance awareness |
| Chief Risk Officer | • Oversee execution of risk management strategies and framework;<br>• Coordinate risk management initiative within the company as per the risk management framework and directives of RMC/ERMSC;<br>• Chair ERMSC meetings and ensure that committee functions as per charter;<br>• Update ERMSC on the key initiatives taken during risk management program;<br>• Oversee the Risk Management Report and relevant documentation;<br>• Monitor risk exposure limits as set by RMC;<br>• Oversee flow of information and escalation of key risk issues/concerns between the RMC and ERMSC of NRL;<br>• Liaise with the Risk Owners and Risk Champions to promote risk aware culture; thereby, ensure transparent reporting of risks;<br>• Ensure that risk register is reviewed and updated periodically (half yearly at minimum);<br>• Present updates / changes to Risk Assessment to the ERMSC on a half yearly basis at minimum for approval |
| ERMSC Members | • Participate in the ERMSC meeting and contribute towards the effective implementation of the ERM framework;<br>• Provide consultation to the ERMSC Chairman to develop and implement risk response plans based on the areas of expertise;<br>• Half Yearly Assessment of identified risks through risk workshops;<br>• Review risk registers, risk reports, and risk statistics to provide independent feedback;<br>• Engage in cross functional forums at the business / operational level to analyse changes in the results of the Company's ERM risk assessment and suggest, implement changes to the reporting and monitoring structure |

| Role | Responsibility |
|---|---|
| **Risk Owners** | • Coordinate the risk management initiative within the department/function as per the risk management framework and the directives of the ERMSC;<br>• Identify, assess, review and monitor risks within department/function assigned to them;<br>• Provide the necessary support to the Risk Champion in the identification, assessment and reporting of risks in his/her area of operation and resolve differences if any;<br>• Participate in meetings for discussion of risks with risk owners of constituent departments/functions;<br>• Perform ongoing assessment of risks and manage existing risks;<br>• Evaluate and validate the status of risk response plans and propose additional controls/response plans (department and enterprise level risks);<br>• Escalate new risks to the ERM Function, so that necessary risk assessments can be conducted, as required;<br>• Ensure that correct and timely risk reports/documentation are maintained and submitted for review and required sign offs obtained |
| **Risk Champion** | • Support Risk Owner through assessment, review and monitoring of risk assigned;<br>• Serve as link between business unit/department and ERM function;<br>• Coordinate risk management activities within department/function;<br>• Provide support to the risk owner in developing risk response plans for department level risks |
| **Employees** | • Understand, adopt, and implement ERM principles across all business operations, projects, and initiatives;<br>• Report any activity which may affect (adversely or positively) strategic objectives of the company;<br>• Participate in the risk management activities by providing best possible information in a timely manner;<br>• Responsible for identifying risks, especially, within their areas of expertise;<br>• Compliance with requests from management in connection with application of the risk management framework;<br>• Exercise care to prevent loss, to maximize opportunity and to ensure that the operations, reputation and assets are not adversely affected. |

(Space left blank intentionally)

## 7.2 RACI Matrix

The above roles and responsibilities of key personnel/groups within the Risk Governance Structure have been condensed into a RACI Matrix as given below:

| Roles & Responsibilities | Board | RMC | ERMSC | CRO | Risk Owner | Risk Champion |
|---|---|---|---|---|---|---|
| Define/Amend Risk Framework comprising of Charter, Policy and Process Manual | I | A | R | I,C | C | C |
| Define Risk Appetite and Tolerance levels | I | A,R | I,C | I,C | C | C |
| Determination of risk impact and likelihood criteria | I | A,R | I,C | I,C | C | C |
| Identify and Evaluate Department Level Risks | - | I | A | A | R | C |
| Aggregate Enterprise Level Risks (Risk Register) | I | A | A | R | C | C |
| Develop Response Plan for Department Level Risks | - | I | I,C | I,C | R | C |
| Develop Response Plan for Enterprise Level Risks | I | A | A,I,C | I,C | R | I,C |
| Monitor Risk Response Plans & Status | I | I | I | A,I,C | R | I,C |
| Oversee Risk Management Reports* | I | A | A | R | I,C | I,C |
| Risk Management Communication | I | I,C | A | R | I | I |

LEGEND:
R- Responsible for undertaking the activity
A- Accountable for making the decisions e.g. Approval etc. for the activity
C- Consulted for input or feedback regarding the activity, agreement not necessarily required
I-Informed about the status of the activity – progress, output or reports

*Key risks (critical/severe) are to be discussed by the Board

(Space left blank intentionally)

## 7.3 Risk Register Template

| # | Risk Category | Business Unit | Risk Statement | CF | IM | LH | RS | RR | EC | RRP | Risk Owner | Primary Impact | Objective |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

CF: Contributing Factors
IM: Impact Score
LH: Likelihood Score
RS: Risk Score
RR: Risk Rating
EC: Existing Controls
RRP: Risk Response Plans

(Space left blank intentionally)

## 7.4 Risk Categories

The following table describes therein the different type of risks based on FORREST Model;

| S. No. | Risk Category | Description |
|---|---|---|
| 1. | Financial | Financial risk is the risk that a firm is unable to meet its financial obligations. It also includes within it, aspects in relation to cost & revenue management, taxation and foreign exchange fluctuation risks.<br><br>E.g.: A higher proportion of debt increases the likelihood that at some point the firm will be unable to make the required interest and principal payments |
| 2. | Operational | Operational risk is the prospect of loss resulting from inadequate or failed procedures, systems or policies. Any event that disrupts business processes is termed as operational risk.<br><br>E.g.: Limited capacity utilization from disruption in crude availability, non- adherence to quality standards, timely execution of scheduled project milestones among others. |
| 3. | Regulatory | Compliance risk is the exposure to legal penalties, financial forfeiture, material loss and reputational impact an organization faces when it fails to act in accordance with industry laws and regulations, local statues, internal policies and procedures and contracts.<br><br>E.g.: Non adherence to environmental statutes resulting in imposition of fines, penalties and probable legal suits against the company |
| 4. | Reputational | Reputational risk is a threat to the goodwill and standing of the organization. It can originate and spread both from inside and outside the organization. The potential for damage from a negative reputation event may take many forms.<br><br>E.g.: Limited brand awareness, Loss of brand confidence due to occurrence of negative events, regulatory scrutiny inviting fines, penalties and possible legal action |
| 5. | Extended Enterprise | These risks pertain to risks originating from third party service providers, vendors, contractors engaged by the organization. It is imperative that these risks are monitored and timely action taken as companies are increasingly being held accountable for the action of third parties.<br><br>E.g.: Financial defaults of contractors inhibiting timely deployment of resources and services, single supplier dependency, confidentiality concerns arising from outsourcing |
| 6. | Strategic | A possible source of loss that might arise from the pursuit of an unsuccessful business plan.<br><br>E.g.: Strategic risk may arise from making poor business decisions, from the substandard execution of decisions, from inadequate resource allocation, or from a failure to respond well to changes in the business environment. |
| 7. | Technological | Risk arising from information technology failures (i.e. hardware or software), inaccurate controls or security of information, vulnerability of system infrastructure, or that a change in technology can create risks within various processes and to service delivery.<br><br>E.g.: Breach in operating systems leading to loss of commercially sensitive data, downtime in critical IT services among other risks. |

## 7.5 Risk Assessment Criteria

The identified risks within the draft risk register needs to be assessed on the basis of their likely "***Impact***" and "***Likelihood***"

**The Impact & Likelihood Assessment Criteria to be employed for risk assessment is as described below;**

a. **Impact Scales:**

The following **risk impact guidance** are meant to help identify the impact that a risk would have on the company. The level of impact may vary depending on the context and situation. The guidance helps to create a level of consistency across the company when categorizing and communicating risk impacts.

| Impact | Description |
|---|---|
| Insignificant (1) | Consequences / event, which can be readily absorbed under routine operating conditions without any visible impact on the organization |
| Minor (2) | Consequences / event, which can be managed under normal operating conditions without additional resources & management effort |
| Moderate (3) | Consequences / event, which can be managed; but, requires additional resources & management effort |
| Severe (4) | Consequences / event which can be endured; but, which may have a prolonged negative impact and alarm the external governing bodies / owners. |
| Catastrophic (5) | Disaster with potential to result in disintegration, thus, challenging the sustainability of the organization and erosion of its values. |

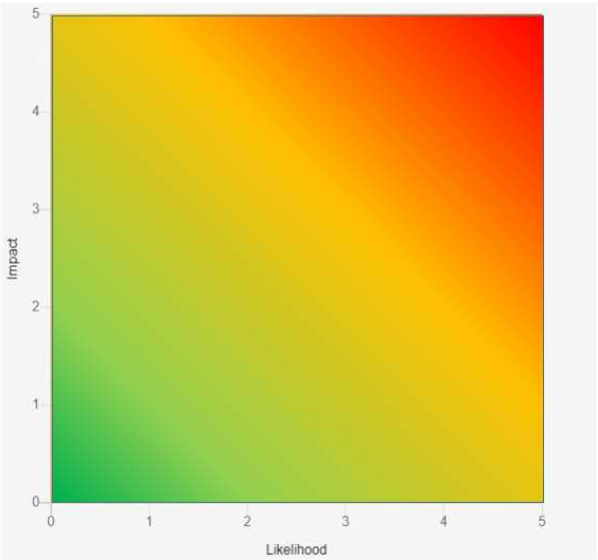
b. **Likelihood Scales:**

The following **risk likelihood guidance** are meant to help identify the likelihood that a risk would occur. The level of likelihood may vary depending on the context and situation. The guidance helps to create a level of consistency across the Company when categorizing and communicating risk likelihoods

| Likelihood | Description |
|---|---|
| Rare (1) | A situation (or an incident) can occur in the rarest of the rare condition |
| Unlikely (2) | A situation (or an incident) had occurred outside the organization, under a rare condition |
| Possible (3) | A situation (or an incident) occurs outside the organization, under the prevailing conditions |
| Likely (4) | The situation (or an incident) may occur within the organization, under prevailing conditions |
| Almost Certain (5) | The situation (or an incident) occurred several times within the organization, under prevailing conditions |

### c. Heat Map and risk criticality to NRL

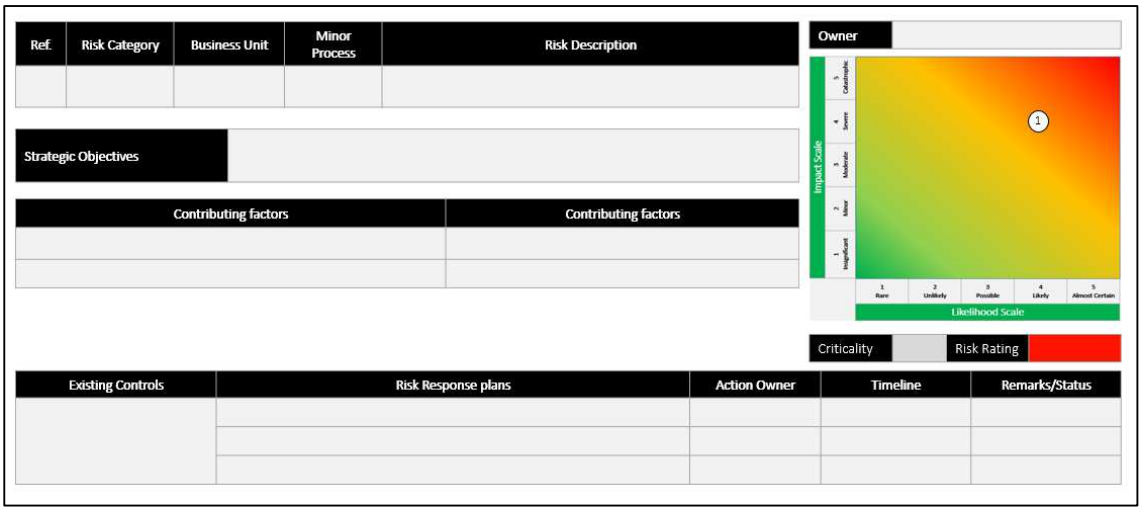
The Risk Score will be computed, i.e. (Risk Impact) * (Risk Likelihood) and accordingly classified into *Severe, Critical, Moderate and Acceptable* by mapping the risks on to a two dimensional matrix called Risk Heat Map as illustrated below;




| Scale | Description of risk criticality |
|---|---|
| Severe | This category of risks possess potential to fundamentally undermine the ability of NRL to perform its core business and achieve strategic objectives. NRL must immediately develop and implement appropriate risk response plans, before continuing the process from which risks are arising. |
| Critical | This category of risks possess potential to adversely impact the strategic objectives of NRL as well as sustain profitable growth. Although, the company can continue to perform its activities from which risks are arising; risk response plans shall be developed and implemented, at the earliest. |
| Moderate | This category of risks may not mandate an immediate attention of management as they possess limited potential to adversely impact operational objectives of NRL. This category is considered equivalent to ALARP 'As Low As Reasonably Practicable' level. NRL should continuously monitor these risks and strive to develop and implement risk response plans, if deemed practicable and economical. |
| Acceptable | This category of risks possess negligible or minimal impact on the organization's performance. NRL should periodically monitor and appraise them to take into account any changes within the internal and external business environment. |

(Space left blank intentionally)

## 7.6 Risk Profile Format




(Space left blank intentionally)

## 7.7 Illustrative Example

### Illustrative example of risk related to Finance:

### 1. Risk Identification

*"Inclusion of MS/HSD under GST and cessation of excise duty exemption benefit may affect the overall profitability of the firm"*

**Contributing Factors for the risk identified is as below:**

1. Refineries in NE region currently enjoy 50% exemption benefit from excise duty payable on manufacture of MS and HSD, that may not be available post transition to GST
2. Changes in the central government policies

Below is an illustration of how the risk so identified is to be updated;

| Risk Category | Business Unit | Risk Statement | Contributing Factors | Existing Controls | Primary Impact | Strategic Objective |
|---|---|---|---|---|---|---|
| Finance | Finance | Inclusion of MS/HSD under GST and cessation of excise duty exemption benefit may affect the overall profitability of the firm | 1. Refineries in NE region currently enjoy 50% exemption benefit from excise duty payable on manufacture of MS and HSD, that may not be available post transition to GST<br>2. Changes in the central government policies | 1. Focus on improvement of Refinery's operational availability and the utilization of refinery complexity including Asset utilization ,turnaround duration reduction, unplanned shutdown avoidance etc. | 1. Erosion of profit margin and resultant hit to GRM due to withdrawal of 50% exemption benefit | Maximization of Gross Refinery Margin and profitability |

### 2. Risk Assessment

Once the risk is identified, the next step is the assessment of the risk. Assessment can be done as per the following steps:

a. Impact Calculation: The risk impact will be calculated based on the severity of impact associated with the risk event. In this case, the risk may challenge the financial and operating sustainability of the organization. Thus, with such a negative impact, the impact of the risk has been scored as "5" (Catastrophic)

b. Risk Likelihood: The Risk Likelihood will be rated as "4" as the said event has may occur within the industry under prevailing conditions (Decision on inclusion of petroleum products to be decided by GST Council and Government of India).

c. Risk Criticality/Score: The risk criticality score will be calculated as the product of Risk Impact and Risk Likelihood. Thus in the above example the risk score will be:

**Risk Score** = Impact (5) * Risk Likelihood (4) = 20.

According to the Risk Criticality and Heat Map defined, this risk will be mapped under "*Severe*" risk category on the heat map. **Example of Risk summarized below:**

| Impact | Likelihood | Risk Score | Risk Rating |
|---|---|---|---|
| 5 | 4 | 20 | Severe |

## 3. Risk Response

Examples for Risk Response Plan for the aforementioned risk;

| Treat | Transfer | Tolerate | Terminate |
|---|---|---|---|
| Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. | Sharing of loss or gain from risk event with another party | Retention or Acceptance of risk is a formal process which Involves accepting the loss, or benefit of gain, from a risk when it occurs. | It is proactive measure to prevent the occurrence of the risk event. |
| E.g. Addition of value added projects and diversification of business - Bio Refinery, wax production Gas JV etc. to reduce dependency on Excise. | E.g. Stream sharing with other refineries. | E.g. Explore ways to increase the yield of high value products | E.g. Basis of existing control, focus on improvement of refinery's operational availability and the utilization of refinery complexity including asset utilization ,turnaround duration reduction, unplanned shutdown avoidance etc. |

Risk is assessed based on existing controls (as defined above in Step 1), subsequent to which response plans are formulated to bring the risk to an acceptable level.

## 4. Risk Review and Reporting

The defined risk will be reviewed by Risk Owner and monitored by Risk Champions. The respective risk registers will be updated and reported as per the defined Risk Governance Structure and Escalation protocols.

## 7.8 Risk Vocabulary

The following risk vocabulary is to be referred to perform all risk management activities:

| Key Terms | Description |
|---|---|
| Management | • Senior CGM's, CGM's, GM's, CM's and division managers- The part of management which is directly involved in handling business operations of the company. |
| Event | • The occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences. |
| Risk | • *"The possibility that events will occur and affect achievement of strategy and business objectives"*<br>• It can also be defined as an *effect* of uncertainty on objectives;<br>• An effect is a deviation from the expected positive and/or negative;<br>• Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, process, and services). |
| Risk Management | • A process, effected by an organization's board of directors, management and other personnel designed to identify potential events that may affect the organization, manage risk within its risk appetite and to provide reasonable assurance regarding the achievement of objectives. |
| Enterprise Risk Management | • The culture, capabilities, and practices, integrated with strategy-setting and its execution that organizations rely on to manage risk in creating, preserving and realizing value.<br>• A systematic approach to provide reasonable assurance to the Board and the stakeholders on risks associated with the organization; including the risk response strategies adopted by the organization in pursuit of organization's objectives |
| Risk Governance Structure | • The Risk Management Process has to be supported by a Risk Governance/Management Structure which primarily comprises of roles and responsibilities to manage risk across the organization. |
| Risk Management Framework | • Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization;<br>• The foundations include the charter, policy comprising of objectives and principles to manage risk; *and*<br>• The organizational arrangements include plans, relationships, accountabilities, resources, processes, and activities. |
| Risk Management Plan | • A scheme within the risk management framework specifying the approach and resources to be applied to the management of risk;<br>• The approach typically include procedures, practices, assignment of responsibilities, sequence, and timing of activities; *and*<br>• The risk management plan can be applied to a particular product/service, process and project, and part or whole of the organization. |

| Key Terms | Description |
|---|---|
| Stakeholder | • A person, organization, or entity that can affect, be affected by, or perceive themselves to be affected by a decision or activity. A decision maker can be a stakeholder. |
| Risk Appetite | • Risk Appetite is the type and amount of risk, on a broad level, an organization is willing to accept in pursuit of value. It established by the RMC for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. |
| Risk Tolerance | • Risk Tolerance is the maximum amount of risk that an organization is able to absorb in the pursuit of strategy and business objectives. |
| Establishing the context | • "Business context" refers to the trends, relationships, and other factors that influence, clarify, or drive change to an organization's current and future strategy and business objectives.<br>• It involves defining the external and internal parameters to be taken into account when managing risk, and setting the scope for implementation of the risk management framework |
| Risk Identification | • The process of determining the risks that could interrupt operations, affect the reasonable expectation of achieving the strategy and business objectives. |
| Risk Source | • It is the element which alone or in combination has the intrinsic potential to give rise to risk |
| Risk Statement | • Risk statement is the description of the risk event(s) along with the likely effect/ impact on the organizational objectives. |
| Contributing Factors | • Contributing factors or Causal factors are the possible proximate causes, which jointly or severally accentuate the chances of the occurrence of a risk event or increase the level of impact of the risk on the organization. |
| Risk Category | • Risks are classified into various categories based on FORREST model (Financial, Operational, Regulatory, Reputational, Extended Enterprise, Strategical and Technological) for better management and control. Each risk category is appropriately defined for the purpose of common understanding. |
| Risk Assessment | • The process of determining the possibility of occurrence of the risk event (Likelihood) and the magnitude of their impact on the organization, which is used to determine risk management priorities basis risk criticality. |
| Impact | • The potential financial and/or non-financial damage experienced by the company in the event of risk materialization and is scored on a scale of 1-5 |
| Likelihood | • It represents the likelihood/probability of the risk materializing and is scored on a scale of 1 – 5 |
| Risk Rating | • The relative rating determined from the Risk Score based on analysis of ***Impact*** and ***Likelihood***. It is categorized as **Severe, Critical, Moderate or Acceptable**. |
| Risk Register | • A Risk Register is a comprehensive record of risks across an organization, department/function/business unit or project depending on the purpose or context of the register, which is detailed with risk statement, contributing factors/causal factors, existing controls, risk response plans, risk owner and risk champion, risk rating among others. |

| Key Terms | Description |
|---|---|
| Key Risk | • Risks which are rated as **Severe/Critical** would be considered as Key Risk and are Board reportable |
| Existing Controls | • Existing controls are the measures, if any, already in place to control the risks. These controls are to be evaluated periodically to ensure they are effective. |
| Response Plans | • Response plan is the process of developing actions to eliminate or reduce the frequency, magnitude, or severity of exposure to risks, or minimization of the potential impact of a threat or warning, in consideration of existing controls |
| Risk Monitoring | • Check, supervise, observe criticality or measure the progress of risk management activity on a regular basis in order to identify change from the performance level required or expected. |
| Risk Reporting | • Form of communication intended to address particular internal or external stakeholders to provide information regarding the current state of risk and its management. |

[Space left blank intentionally]

## 7.9 Summary Chart

A summary chart displaying the activities to be followed periodically is given below:

| Roles | Periodicity of Meeting | Activities | |
|---|---|---|---|
| | | Half Yearly | Yearly |
| Risk Owner | - | - Identify and Evaluate Department and Enterprise Level Risks<br>- Develop Response Plan for Department and Enterprise Level Risks | - |
| Chief Risk Officer | - | - Consulted for Response Plan for Enterprise Level Risks<br>- Co-ordinate to update the consolidated risk register<br>- Present the consolidated risk register before the ERMSC | - Present critical risks and their risk profiles as identified by ERMSC to the Board<br>- Oversee the Risk Management Reports |
| ERMSC | Half Yearly | - Aggregate and assess the Enterprise Level Risks during the risk workshops<br>- Determine the Board reportable risks and track the progress of the risk response plan for the same | - Finalise the risk management report |
| Risk Management Committee (RMC) | Yearly | - | - Review of corporate and key/critical risks reportable to the board & their Risk Profiles<br>- Set the risk appetite and tolerance levels<br>- Review of the risk assessment criteria |
| Audit Committee / Board of Directors | Yearly | - | - Review of key/critical risk areas<br>- Oversee the progress of ERM implementation |