Petronet LNG Limited

Risk Management Policy and Procedures

Rev.-03

Revision	Approval Date	Remarks
3	9th November, 2021	Policy revised based on SEBI Circular dated 05-05-2021
2	8th November, 2019	Policy revised
1	2015	Minor change in RMC composition.
0	17th October, 2006	Risk Management Policy & Procedures implemented

Abbreviations

PLL:	Petronet LNG Limited
HOD:	Head of the Department
RMC:	Risk Management Committee
CRO:	Chief Risk Officer
VP:	Vice President

Table of contents

1. Introduction

A risk is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk includes all events, actions or omissions, internal or external, which have the potential to threaten the success or even the survival of the Company. Risk is not restricted to unexpected negative developments but also to the missing or removal of positive developments and opportunities. Risks are inevitable, as there can be no entrepreneurial activity without the acceptance of risks and associated profit opportunities.

This risk management policy ("the policy") outlines the risk management framework for Petronet LNG Limited ("PLL"). PLL considers good corporate governance as a pre- requisite for meeting the needs and aspirations of its shareholders and other stake holders in the company.

The policy is intended to ensure that an effective risk management program is established and implemented within PLL and to provide regular reports on the performance of that program, including any exceptions, to the Board of Directors of PLL, Audit Committee and the Risk Management Committee.

The policy contains the purpose of risk management, PLL's approach to risk management and the risk organization structure for identification, escalation, and minimization of risks. The policy also specifies the roles and responsibilities of the Board of Directors, Audit Committee and other key personnel of the company with regards to risk management.

The policy complements and does not replace other existing compliance programs, such as those relating to environmental, quality, and regulatory compliance matters.

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives

*(As defined by Committee of Sponsoring Organizations of the Treadway Commission **(COSO) ERM Framework 2004**)*

2. Purpose of Risk Management

The purpose of Risk management in PLL is to identify and manage risks that may impact the achievement of following key business objectives:

- Sustain business growth
- Protect the company's assets
- Minimize operational surprises and losses
- Safeguard shareholder interests
- Ensure compliance with applicable legal requirements.

Risk management activities at PLL are not aimed at eliminating all risks in their entirety, but rather at helping to identify and assess the risks the Company encounters in its daily business. This allows the Company to manage the risks in an efficient manner to take informed decisions, to exploit the opportunities available and thereby enhance the value of the Company and its stake holders.

3. Applicability

This policy applies to all employees of PLL and every part of PLL operations and functions.

4. Objectives of Risk Management

Risk Management objectives of PLL are as follows:

- To identify, assess and manage existing as well as new risks in a planned and coordinated manner.
- To increase the effectiveness of PLL's internal and external reporting structure.
- To develop a "risk" culture that encourages all staff to identify risks and associated opportunities and respond to them with appropriate actions.

To realize these Risk Management Objectives, PLL aims to ensure:

- Identification and assessment of key risks in the context of the company's risk appetite.
- Continuous monitoring and management to an acceptable level of the potential impact of risks.
- Accurate, complete and timely escalation of risk information to support management decision making at all levels.
- Active involvement of all employees in the risk management process within their own areas of responsibility.

5. Risk Management Strategy

The Risk Management Strategy is developed and approved by the top management and is

significantly influenced by the regulatory requirements. The strategy is implemented by developing a risk management structure, policies and procedures.

6. Risk Portfolio Management

Risk management is a continuous cycle beginning with risk identification and followed sequentially by risk assessment, addition to the risk register, control assessment, risk review and risk escalation.

Head of Departments must periodically review the risks facing their department in line with the risk management process. This review should include identifying all significant risks.

Each manager must then implement an effective system of internal controls to manage those risks, including most importantly designating responsibilities, and providing for upward communication of any significant issues that arise.

Risk identification and management is a continuous process supported by formal reviews conducted on quarterly basis.

The Risk Management process flow is detailed in **Annexure 1**.

6.1 Risk Identification

The identification of risks is the first step in the risk portfolio management. Risk identification must begin with understanding the objectives of PLL that the process owners are responsible to achieve and the strategies that have been adopted to achieve organizational objectives. The purpose of identification of risks is to identify the events that have an adverse impact on the achievement of the business objectives.

In order to identify risks, a range of potential events will be considered while taking into account past events and trends as well as future exposures.

An event identified may have negative or positive impact. An event with positive impacts represents an opportunity and an event with a negative impact represents a risk. Risks identified may be of the following types:

- Strategic Risk
- Operational Risk
- Reputation Risk
- Compliance Risk
- Financial Risk
- Information Risk
- Other Risk

A brief description of factors to be considered for categorization of risks is detailed in **Annexure 2.**

Procedure:

Each Head of Department is responsible for identification of risk within his sphere of responsibility. Besides identification of risks, the departmental heads also identifies controls currently in place to mitigate the risks identified, as well as additional controls to be put in place, if required.

The Chief Risk Officer (CRO) actively assists departmental heads in identification of risks. Formal record of new risks identified is maintained by the departmental heads.

6.2 Risk Assessment

Risk assessment involves analysis of identified risks and quantification of the impact of risks to determine its potential severity and the probability of occurrence of the risk to determine its potential frequency.

The objective of the risk assessment exercise is to measure relative importance of risks to facilitate prioritized decision making.

Each identified risk is assessed on a 5 point scale with respect to the following criteria for determining inherent and residual exposure:

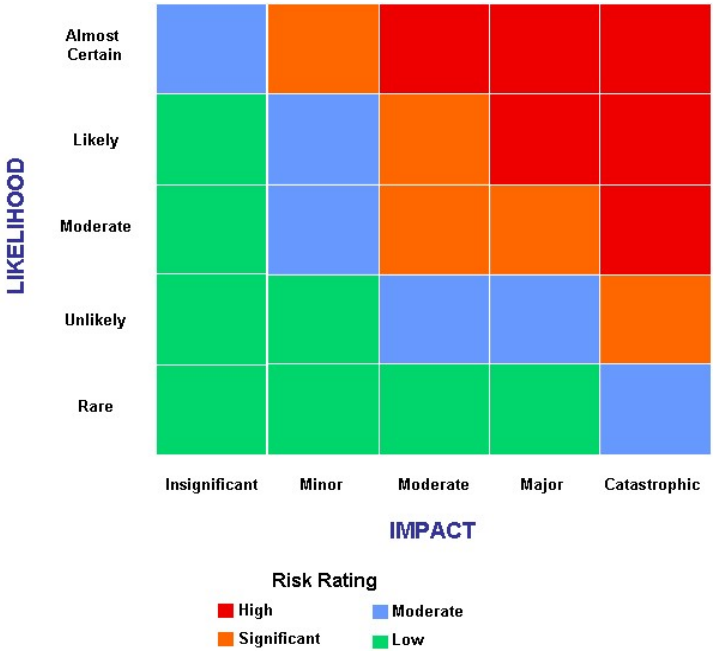
a) Likelihood of event occurrence

b) Impact if the event occurs

Both inherent and residual risks are to be considered in the process of risk assessment. Inherent risk is defined as the risk faced by the organization in the absence of any actions that management might take to alter the risk's impact or likelihood. The combination of likelihood of event occurrence and impact provides the inherent risk exposure.

The components of gross risk i.e. the probability of occurrence and magnitude of impact are sought to be altered by putting in place certain controls. The risk that remains after the controls are put in place is termed as residual risk. The combination of residual likelihood and residual impact provides the residual risk exposure. The Risk Appetite has been detailed in **Annexure 3**.

The Risk Assessment Table below depicts the risk exposure:



6.2.1 Risk Optimization

Risk Optimization involves managing the exposure of various risks and bringing them in line with the risk appetite of the company. Options for risk optimization include:

Risk Acceptance: Risks which cannot be avoided, reduced or transferred are to be accepted by the company.

Risk Avoidance: Risks whose likelihood, consequences or organizational impact is significant hence management may choose to avoid them altogether.

Risk Mitigation: It is an approach to reduce either the likelihood or the consequences of the risk event.

Risk Transfer: Transferring means soliciting the involvement of a third party to take on the impact should a risk event occur.

Procedure:

Identified risks, risk ratings, controls and action plans, as well as modifications and deletions are forwarded by the respective Head of Department to the Chief Risk Officer, who will collate all the risks and present the same to the Risk Management Committee (RMC) on a quarterly basis for review and approval.

Annual Risk Assessment for strategic risks is done by the Board.

6.3 Updation of Risk Register

The purpose of the Risk Register is to record the risks identified and acts as a central repository of risks. Reports drawn from the register are used to communicate the current status of all known risks and are vital for assessing management control, reporting and reviewing the risks faced by PLL.

The Risk Register contains the following information with respect to each identified risk: Risk Description, Risk Owner, Root Causes, Risk Category, Key Performance Indicators, Inherent Risk Evaluation, Controls to mitigate the risk, Residual Risk Evaluation, Action Plan, Owner, Timelines and status of action plan.

Procedure:

Risks, risk ratings, controls and action plans ratified by the RMC are incorporated in the Risk Register.

Risk Register is centrally maintained by a person designated by the CRO, and all additions/ deletions/ modifications to the Risk Register are made after obtaining approval of the Risk Management Committee.

6.4 Risk Monitoring, Review and Communication

All risks recorded in the risk register are re-assessed to ensure that the risk assessments as currently recorded remain valid.

Risk review also involves the following:

1. Assessment of completeness and validity of risks recorded in the risk register
2. Assessment of changes in the business processes, operating and regulatory environment since the last risk assessment and corresponding changes required in the risk profile, risk appetite and risk management procedures of the organization.
3. Reviewing efficacy and implementation status of actions plans for identified risks and revision in action plans.
4. If the risk gets triggered, responsible person shall share the action plan with CRO.

5. All risk has to be monitored by Functional Head and his superiors depending on severity of risk. Level of Superior is defined as following:

- Low Risk: Functional Head
- Moderate Risk: One level above Functional Head or VP whoever is senior
- Significant Risk: Functional Director
- High Risk: Managing Director & CEO

Procedure:

Status of implementation of action plans is reported and monitored by concerned HOD and CRO. Further, the CRO provides quarterly updates to the Risk Management Committee (RMC) for key risks (High & Significant risks), their assessment and status of action plans for mitigating these risks.

RMC in turn updates the Board / Audit committee on a quarterly basis.

7. Risk Organization Structure

The Risk Management Structure is detailed in **Annexure 4**.

7.1 Roles and Responsibilities

Formal authority, responsibility and accountability for designing, implementing and sustaining effective risk management processes rests with the Board of Directors. The Risk Management Committee, management and other employees support and assist the Board of Directors in fulfilment of this responsibility.

The risk management roles and responsibility are detailed in **Annexure 5**.

7.2 Risk Management Committee (RMC)

7.2.1 Composition

The composition of RMC shall be as per RMC charter.

In addition, the RMC may invite other personnel to attend the RMC meetings as required.

7.2.2 Frequency of Meetings

The RMC shall ordinarily meet on a periodic basis as defined in Risk Management Committee Charter to review risks or to review other matters. The agendas and the minutes of the meetings of RMC shall be recorded and maintained by the Secretary to the RMC.

7.2.3 Deleted, Amended and Merged with Annexure 5.

8. Validity of the Policy

The policy is valid indefinitely in its entirety unless amended by the same approving authority.

9. Glossary of Terms

1. **Control:** Any action taken by the management, the Board, and other parties to manage risk, and increase the

likelihood that established objectives and goals will be achieved.

2. **Enterprise Risk Management:** A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that effect the achievement of its objectives.

3. **Inherent Risk:** The risk prevailing in the activity before the implementation of controls

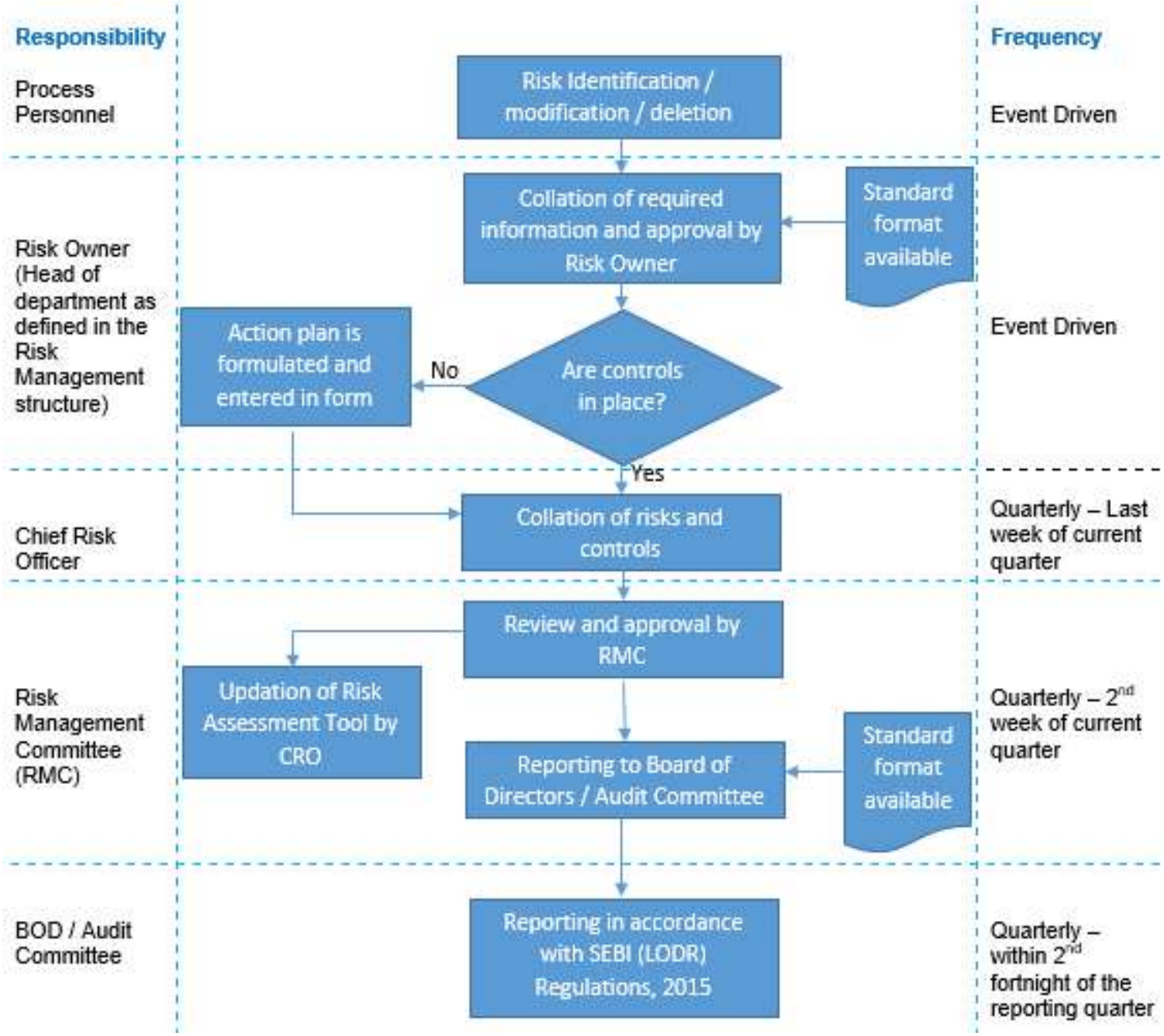
4. **Risk:** The possibility of an event occurring that will have an impact on the achievements of the objectives. Risk is measured in terms of impact and likelihood.

5. **Risk Appetite:** The Level of risk that is acceptable to the management. This may be set in relation to the organization as a whole, for different group of risks or at an individual risk level.

6. **Risk Management Process**: Processes to identify, assess, manage and control potential events and situations, to provide reasonable assurance regarding achievement of organizational objective.

10. Annexure

Annexure 1 – Risk Management process flow



1. Format for Risk identification / Modification / Deletion

Petronet LNG Limited										
Format for Risk identification / Modification / Deletion										
Risk ID	Risk Category	Risk Description	Trigger Point	Potential Root Cause	Risk Rating				Risk Owner	Change Type (Add / Modify / Delete)
					Impact	Likelihood	Risk Score	Risk Rating		

2. Format for reporting to Board of Directors / Audit Committee

Petronet LNG Limited														
Format for reporting of risks to BOD														
Risk ID	Risk Category	Risk Description	Trigger Point	Potential Root Causes	Risk Rating				Existing Mitigating Factors	Future Action Plan	Risk Owner	Action Plan Owner	Monitored By	Target Date
					Impact	Likelihood	Risk Score	Risk Rating						

Annexure 2– Risk Categorization

Identifying and Assessing Risk	
Factors to be considered by the Board during risk identification and assessment	
Strategic Risk	./ Are the critical strategies appropriate to enable the organization to meet its business objectives? ./ What are the risks inherent in those strategies, and how might the organization identify, quantify, and manage these risks? ./ How much risk is the organization willing to take?
Operational Risk	./ What are the risks inherent in the processes that have been chosen to implement the strategies? ./ How does the organization identify, quantify, and manage these risks given its appetite for risk? How does it adapt its activities as strategies and processes change?
Reputation Risk	./ What are the risks to brand and reputation inherent in how the organization executes its strategies?
Compliance Risk	./ What risks are related to compliance with regulations or contractual arrangements —not just those that are financially based?
Financial Risk	./ Have operating processes put financial resources at undue risk? ./ Has the organization incurred unreasonable liabilities to support operating processes? ./ Has the organization succeeded in meeting business objectives?
Information Risk	./ Is our data/information/knowledge reliable, relevant, and timely? ./ Are our information systems reliable?
New / Other Risk	./ What risks have yet to develop? (These might include risks from new competitors or emerging business models, recession risks, relationship risks, outsourcing risks, political or criminal risks, financial risk disasters (rogue traders), and other crisis and disaster risks.)

Annexure 3 – Risk Appetite

Rating Criteria - Impact

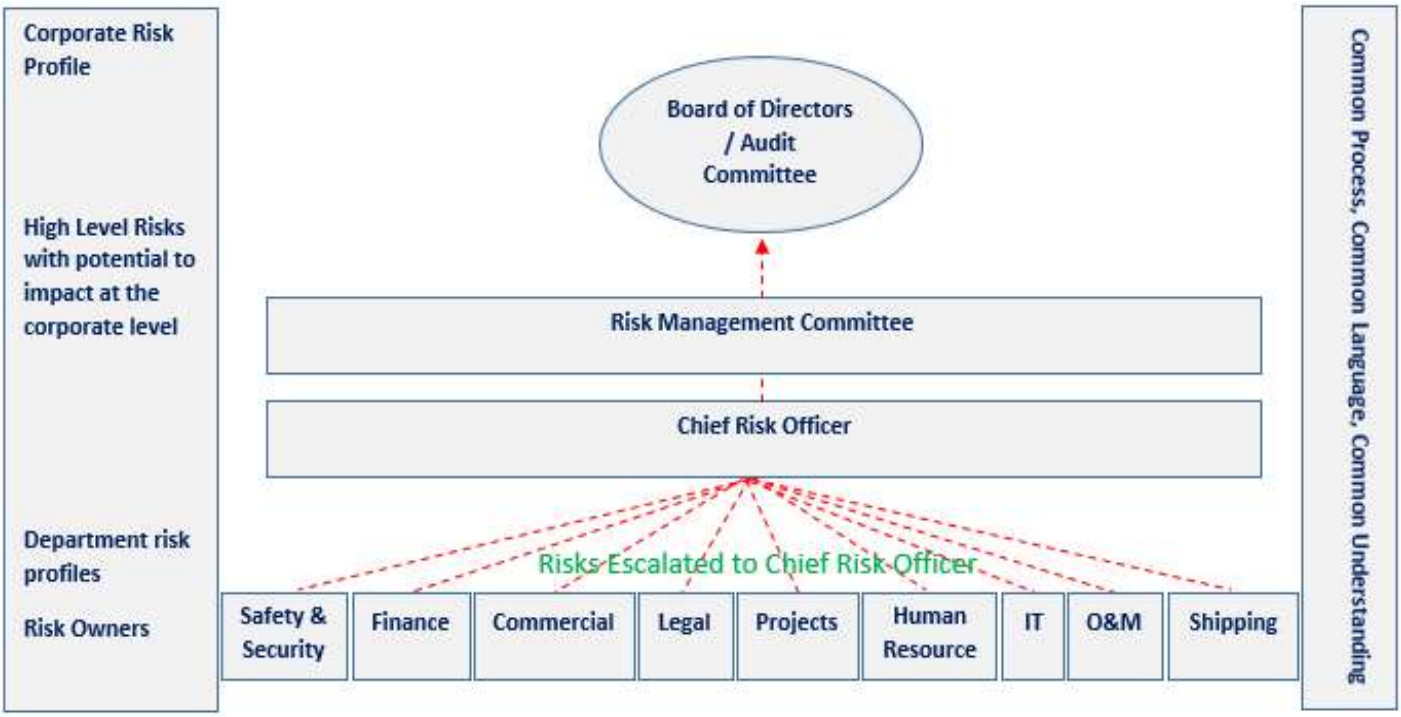
Criteria	Criterion Description	Insignific ant	Minor	Moderate	Major	Critical
	Impact Score	1	2	3	4	5
Capacity Utilization	Reduction in capacity utilization	Less than 0.5% on capacity utilization	0.5 to 1%	1 to 2%	2 to 3%	Greater than 3%
Financial (Profitability)	Impact on annual profitability (PBDIT)	Less than 0.5% on PBDIT	0.5 to 1%	1 to 2%	2 to 3%	Greater than 3%
Delay in completion of Projects	Delay in completion of projects from schedule timelines	Delay upto 2% of project duration	Delay from 2 to 5% of project duration	Delay from 5 to 10% of project duration	Delay from 10 to 15% of project duration	Delay of more than 15% of project duration
Plant operations (days lost on due to disruptions)	Interruption in operations	< 6 hours	6-12 hours	12-24 hours	1-2 days	> 2 days, on account of interruptions, closure of manufacturin g facility
Health, Safety, Security / property damage	Loss of life and property due to accidents/ thefts	Physical discomfort / damage upto INR 10,000	First aid case / damage of INR 10,000 to 1 lakh	Temporary disability or medical treatment case / damage of 1 to 50 lacs	Permanent disability or Lost work incident / damage of 50 to 100 lacs	Fatality / damage more than 100 lacs
Environmental	Ecological loss due to non compliance with environmental norms	Negligible effect confined to plant	Minor impact to ecosystem. Damage recoverable through short term measure within 2-3 days	Temporary localised effect on ecosystem for which rectification is required over a week. Reportable to regulatory authorities	Major temporary effect on ecosystem for which rectification is required over a month. Potential fines by regulatory authorities	Major permanent effect on ecosystem for which rectification is unlikely
Regulatory compliance	Penalties imposed by regulatory authorities	Routine issues raised by Ministry / regulatory authorities	Warning letter received from statutory authorities	Penalties levied by statutory authorities between INR 1 to INR 50 lacs	Penalties levied by statutory authorities between INR 50 lacs to 100 lacs	Penalties levied by statutory authorities of greater than 100 lacs Possibility of imprisonmen t of director(s)

Criteria	Criterion Description	Insignific ant	Minor	Moderate	Major	Critical
	Impact Score	1	2	3	4	5
Interventions	Level of escalations	Departme nt Head	Department VP/ President	Director	Managing Director	Board of Directors
Loss of Key Alliances (Vendors / Customers)	(Key vendor / customer is defined as an entity from which the company procures / sells at least 1% of the total spent / turnover during a year)	Loss of 1 non-key alliance	Loss of multiple non-key alliance	Loss of multiple non-key alliance amounting to <= 1% of total spent / turnover	Loss of one key alliance or multiple non-key alliances amounting to 1 to 5% of total spent / turnover	Loss of alliances affecting > 5% of total spent / turnover
Attrition % at the following levels: Senior Management ("SM") Middle Management ("MM") Lower Management ("LM")	Average attrition over last 3 years	SM: No Person MM: No Person LM: 1-3%	SM: No Person MM: <= 1% LM: 3-5%	SM: No Person MM: 1-3% LM: 5-7%	SM:1 Person MM: 3-5% LM: 7-9%	SM: >1 Person MM: >5% LM: >9%

Rating Criteria - Likelihood

Particular	Criterion Description	Almost certain	Likely to happen	Moderate	Low	Remote
	Likelihood Score	5	4	3	2	1
Likelihood Criterion	Probability	Within 12 months	1 - 3 years	3 - 5 years	5 - 7 years	7-10 Years
	Occurence	Event is certain to occur in most circumstances	High probability for the event to occur	Event should occur sometime	Event may occur in exceptional situations	Possibility of occurrence of event is remote

Annexure 4 – Risk Organization Structure



Annexure 5 – Roles and Responsibilities

Category	Description of Roles and Responsibilities
Board of Directors	Approve risk policy and risk management approach Define Risk Appetite for the company Review of organization risk portfolio and considering it against the risk appetite Supports an environment that does not tolerate behaviour which might compromise prudent risk management practice Present Board Disclosures as mandated by SEBI (LODR) Regulations, 2015 on risk management to stock exchanges/ SEBI Review of RMC Charter from time to time so as to ensure it remains consistent with the Committee's authority, objectives and responsibilities Approval of amendment to the RMC Charter
Risk Management Committee (RMC)	1. To highlight significant changes in the risk profile, changes/events outside the risk appetite of the company. 2. To provide leadership and direction to the company on the Risk Management framework. 3. To develop a framework for identification of internal and external risks specifically faced by the company, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks, Business Continuity Plan (BCP) or any other risk as may be determined by the Committee. 4. To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;

	5. To ensure that appropriate methodology/measures including systems and processes of internal control are in place to monitor, evaluate & mitigate risks associated with the business of the Company. 6. a) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken b) To submit reports as desired by the Audit Committee/Board of Directors on changes in risk profile, controls established, etc. 7. To communicate summary of changes in risk register to the Audit Committee / Board of Directors of the Company. 8. To review the management of the risk, their root causes and the control to mitigate the risk. 9. To review modifications, additions and deletions to the Risk Register 10. Monitor emerging issues and share best practices.
	11. Ensure validity and completeness of the risk assessment tool 12. Performance of duties and assumption of responsibilities as per RMC charter 13. Any other matter as decided by the Board of Directors of the Company or as specified under the provisions of Companies Act, 2013 and SEBI (LODR) Regulations, 2015 as amended from time to time. 14. The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee. 15. 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.

Category	Description of Roles and Responsibilities
Chief Risk Officer (CRO)	Special invitee of Risk Management Committee Framing accountability and authority for risk management Promoting risk management competence throughout the entity, including facilitating development of technical risk management expertise and helping managers align risk responses with the entity's risk tolerances Guiding integration of risk management with other business planning and management activities. Establishing a common risk management language that includes common measures around likelihood and impact, and common risk categories Overseeing development of risk tolerances and working with managers to establish control activities and recommending corrective action where needed Collate updates/ changes from respective process owners Update Risk Assessment Tool Present MIS to the RMC periodically
Head of Departments	Guiding and monitoring application of enterprise risk management within their spheres of responsibility Identification of additions and modifications to existing risk register Carrying out risk rating and categorization Responsible for execution of action plans for risk mitigation Identification of controls and action plans and review of their efficacy and application Reporting of risks to the Chief Risk Officer (CRO)
Employees	Compliance with risk policy requirements and management directives Identification of divisional risks Exercise reasonable care to prevent loss, to maximize opportunity and to ensure that the operations, reputation and assets are not adversely affected