Petronet LNG Limited

Integrated Risk Management and Business Continuity Policy

Rev-04

Revision	Approval date	Remarks
4	19 March 2025	Risk Management Policy as per ISO 31000 along with Business Continuity Management Policy as per ISO 22301
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

Petronet LNG

Integrated Risk Management and Business Continuity Procedures

Risk Management Policy

PLL is committed to manage uncertainties and associated business risks through development and implementation of a well-defined Risk Management Framework, which provide for identifying, assessing, mitigating, monitoring, evaluating, and reporting of all risks, including IT and Fraud Risk and associated opportunities on a continuous basis for sustained growth.

Systematic monitoring and effective course corrections will be undertaken to achieve organization's business objectives and optimize associated risk exposure in line with acceptable risk appetite.

(For detailed policy refer Annexure 1)

Business Continuity Policy

To ensure uninterrupted services, PLL is committed to implement a robust business continuity management system aligned with the global standard of ISO 22301:2019 and industry best practices. This policy aims to foster a culture of resilience and preparedness, by identifying, preventing, minimizing, and managing the impact of disruptive events and ensuring continuous delivery of critical services and business operations even in the face of such unexpected events. This policy shall serve as a guiding document for all employees, stakeholders, and third-party vendors, emphasizing the importance of business continuity management in maintaining service integrity. This policy provides guidance on the development of BCM framework to be followed across PLL, in line with ISO 22301:2019 requirements.

(For detailed policy refer Annexure 2)

Annexure 1:

RISK MANAGEMENT POLICY

Table of Contents

RISK MANAGEMENT POLICY

INTRODUCTION

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.

This policy adopts the approach used in ISO 31000:2018 Risk management – Guidelines and identifies the importance and relevance of ISO 31000. Risk is the “effect of uncertainty on objectives” and an effect is a positive or negative deviation from what is expected. Negative deviations are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization’s business objectives. The exposure to the consequences of uncertainty constitutes a risk.

Organizations, irrespective of their type and size, contend with internal and external factors that introduce uncertainty regarding the realization of their business objectives. In recent years, there has been a widespread shift across all sectors of the economy towards prioritizing risk management as the linchpin for organizational success in achieving objectives while safeguarding stakeholder interests. Those organizations demonstrating effectiveness and efficiency in managing risks, be it for existing assets or future growth, are poised to outperform their counterparts over the long term. In essence, companies accrue profits through judicious risk-taking and incur losses when they fail to manage risks intelligently.

Risk management is a comprehensive, integrated, structured, and disciplined approach aimed at proactively handling uncertainties with the goal of maximizing stakeholder value. This approach aligns strategy, processes, people, culture, technology, and governance to systematically evaluate and manage uncertainties faced by the organization while simultaneously creating and safeguarding value. With the vision to integrate risk management with the overall strategic and operational practices, an Enterprise Risk Management Framework has been established by PLL, as a comprehensive set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

The revised policy also aims at establishing responsibility towards review of procedures, processes in place to ensure alignment with changes in Companies Act, 2013 and applicable amendments, SEBI’s LODR (Listing Obligations and Disclosure Regulations, 2015) requirements, financials, business volumes, qualitative parameters, and other applicable parameters.

GLOSSARY

Company/Organization: Petronet LNG Limited (PLL)

Chief Risk Officer (CRO): CRO is a senior executive who manages an organization's risks by playing a pivotal role in the oversight and execution of company's risk management function.

Board of Directors / Board: As per Section 2 of "The Companies Act, 2013", in relation to a Company, means the collective body of Directors of the Company.

Enterprise Risk Management (ERM): The risk management process involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk.

Risk: 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. Negative deviations are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. The exposure to the consequences of uncertainty constitutes a risk.

Risk Management: Risk management can be defined as the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risk management framework: Risk Management Framework (RMF) is the structured process used to identify potential threats to an organization and to define the strategy for eliminating or minimizing the impact of these risks, as well as the mechanisms to effectively monitor and evaluate this strategy.

Risk Management Committee: RMC review the exception reports along with effectiveness of the mitigation plans and the approval for inclusion/deletion of new risks and modification of the mitigation plans.

Risk Steering Committee: The Risk Steering Committee (RSC) is responsible for providing inputs to Risk Management Committee (RMC) including moderation of responses shared by Risk Controllers on Bi-annual basis. RSC may share feedback on case-to-case basis with Risk Controllers and thereafter with RMC.

Risk Controller: Risk control is a step in the hazard management process. It involves finding a way to neutralize or reduce an identified risk. Risk Controller would be a functional level person across PLL responsible for moderating responses shared by Risk Owners at a quarterly frequency. The controller would provide feedback to risk owners and share output with RSC.

Risk owner: A risk owner is an accountable point of contact for an enterprise risk at the senior leadership level, who coordinates efforts to mitigate and manage the risk with various individuals who own parts of the risk.

Risk Repository: Risk repository contains those risks which are not a part of the ERM risks as of now due to strengthened mitigation measures or its impact and likelihood are not significant in nature. If any of these risks trigger to an ERM level magnitude, it can be taken up to the ERM risk register through change management process.

Inherent Risk: Risk level before introduction of any mitigating controls

Residual Risk: Risk level post introduction of mitigating control activities

Events: An event is an occurrence or change of a particular set of circumstances. An event can potentially be a risk source.

Risk Score: Risk score is a calculated number (score) that reflects the severity of a risk.

Risk Criteria: Risk criteria are terms of reference and are used to evaluate the significance or importance of the organization's risks.

Risk Register (Risk Reports): A prioritized compilation under all PLL Business Units highlighting the risks for the company.

Impact: The degree of consequences to the organization should the event occur. [Refer to impact scale criteria definitions – Appendix 1]

Likelihood: The likelihood of the event occurring expressed as an indicative annual frequency. [Refer to likelihood scale criteria definitions – Appendix 1]

Consequence: The effect, result, or outcome of a potential risk.

Risk Source: Element which alone or in combination has the intrinsic potential to give rise to risk.

Risk Rating: The relative rating determined from the risk score derived from qualitative analysis of impact and likelihood. Categorized as High, Medium, or Low. [Refer to Risk Rating definitions – Appendix 1]

Risk Exposure: Risk exposure is the measure of potential future loss resulting from a specific activity or event.

Risk Appetite: Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of objectives.

Uncertainty: Uncertainties are inherent in all scientific undertakings and cannot be avoided. Proactively managing uncertainties leads to value addition for the company.

Threat: Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Risk Treatment: A risk treatment is an action that is taken to manage a risk.

Mitigation: Risk mitigation is defined as taking steps to reduce adverse effects.

Risk Identification: Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives.

Risk Analysis: Risk analysis is the process of identifying and analyzing potential issues that could negatively impact key business initiatives or critical projects in order to help organizations avoid or mitigate those risks.

Risk Evaluation: Risk evaluation is the process of identifying and measuring risk.

Risk Response: The mitigation measures taken by an organization to deal with a risk.

1.0 POLICY STATEMENT PERTAINING TO RISK MANAGEMENT

PLL recognizes that it is exposed to a number of uncertainties, which is inherent for the energy sector that it operates in. To be in line with ISO 31000 requirements, PLL is committed to proactively managing uncertainties, not only to mitigate risks but also to enhance the organization's value by facilitating the efficient achievement of its objectives. The policy statement aims at:

A. Establishing a comprehensive and integrated Risk Management Framework, encompassing the identification, assessment, mitigation, monitoring, evaluation, and reporting of all risks, with a specific focus on IT and Cyber Risks.

B. Provide a clear and robust foundation for informed decision-making at all organizational levels.

C. Foster a continuous enhancement of the Risk Management System through ongoing learning and improvement, ensuring the successful realization of policy objectives through diligent implementation and monitoring.

D. Identify and proactively manage newly emerging risks effectively.

E. Minimize risks to the greatest extent possible by strategically managing their exposure and aligning them with the acceptable risk appetite of the company.

F. Implement and maintain effective systems to achieve policy objectives through systematic monitoring, incorporating timely course corrections as needed.

1.1 Requirement as per Companies Act, 2013

Responsibility of the Board: As per Section 134 (n) of the Act, the board of directors' report must include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the Company.
Responsibility of the Audit Committee: As per Section 177 (4)(vii) of the Act, the Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include evaluation of internal financial controls and risk management systems.
Responsibility of the Independent Directors: As per Schedule IV [Part II-(4)] of the Act, Independent directors should satisfy themselves that financial controls and the systems of risk management are robust and defensible.

1.2 Requirement as per SEBI (Listing Obligations and Disclosure requirement's), Regulation 2015

The company through its Board of Directors shall constitute a Risk Management Committee. The Board shall define the roles and responsibilities of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit.

A. Regulation 4: Key function of the board of directors is to ensure the integrity of the listed entity's accounting and financial reporting systems, including the independent audit & that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control and compliance with law and relevant standards.
B. Regulation 17: Board of Directors shall be responsible for framing, implementing, and monitoring risk management plan of listed entity.
C. Listed entity shall lay down procedures to inform members of board of directors about risk

assessment and minimization procedures.

D. Regulation 18: Audit Committee need to evaluate the internal financial controls and risk management systems.

E. Regulation 21: Board of Directors have been casted with a responsibility of formulating a Risk Management Committee which shall be charged with monitoring and reviewing of the risk management plan.

1.3 Objectives of the Policy

The main objective of this policy is to ensure sustainable business growth with stability and to promote a pro-active approach in identifying, evaluating, reporting, and managing risks associated with the business. In order to achieve the key business objectives, the policy establishes a structured and disciplined approach to Risk Management, including the development of Risk Register, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are, to:

A. Ensure thorough identification, assessment, mitigation, monitoring, and reporting of all current and future material risk exposures of the company.

B. Establish a comprehensive framework for the company's risk management process, ensuring widespread implementation throughout the organization.

C. Facilitate compliance with relevant regulations by adopting best practices across the company.

D. Ensure business growth coupled with financial stability.

E. Ensure the effectiveness of Risk Mitigation plans through rigorous monitoring and evaluation of outcomes. Explore opportunities to apply successful mitigation strategies to other areas, contributing to the overarching objectives of this policy.

To attain these objectives, PLL will uphold the following core principles:

A. **Effective Risk Management Process:** The Board-appointed Risk Management Committee will bear the overarching responsibility for ensuring an effective risk management process within the company.

B. **Everyone’s Commitment:** Every function, department, and office within the organization will collaborate to ensure the seamless implementation of this risk management policy.

C. **Proactive Leadership:** Ongoing activities such as risk identification (including the identification of potential missed opportunities), key risk assessment, risk response, and risk monitoring will be integral to the company's operations, management, and decision-making processes. All identified risks will be regularly updated in a centralized repository.

D. **Risk Culture:** Informed and consistent decisions regarding risks will be made, non-compliant behaviors will not be tolerated, and the management of risks will be conducted in a professional manner.

E. **Transparency and Compliance:** The organization will report on risk management activities, highlighting the most significant risks. Material failures in mitigation measures will be escalated through the reporting line to the relevant levels of the organizational structure.

F. **Result Evaluation:** Regular assessments will be conducted to evaluate the effectiveness of the Risk Management Policy and its implementation, identifying areas for improvement as needed.

1.4 Scope and Applicability of the Policy

This policy applies to all employees of PLL and extends to every facet of PLL's operations and functions.

2.0 THE RISK MANAGEMENT FRAMEWORK

Risk management will protect and add value to the organization and its stakeholders through supporting the organization's objectives by improving decision making, planning and prioritization by comprehensive and structured understanding of business activity, volatility, and project opportunity/threat. It will provide a framework that enables activity to take place in a consistent and controlled manner. The framework will help in creating an environment in which risk management is consistently practiced across the Company and where Management can take informed decisions to reduce the possibility of negative events. The components of risk management are defined by the company's business model and strategies, organizational structure, culture, risk category and dedicated resources. An effective risk management framework requires consistent processes for assessment, mitigation, monitoring and communication of risk issues across the organization. Essential to this process is its alignment with corporate direction and objectives, specifically strategic planning, and annual business planning processes. Risk management is a continuous and evolving process, which integrates with the culture of the Company.

An effective Risk Management Framework comprises of:

- Risk management process; and
- Risk management organization structure

Risk management Process can be defined as the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risk Management Organization Structure: The risk management process has to be supported by a risk management structure which primarily comprises of:

- Team structure of the Risk Management Function
- Roles and Responsibilities
- Risk management activity calendar

2.1 The Risk Management Approach at PLL

PLL has adopted a comprehensive Enterprise Risk Management (ERM) approach across the entire value chain to identify and manage risks at the overall entity level. The risk methodology adopted has the following two facets to it:

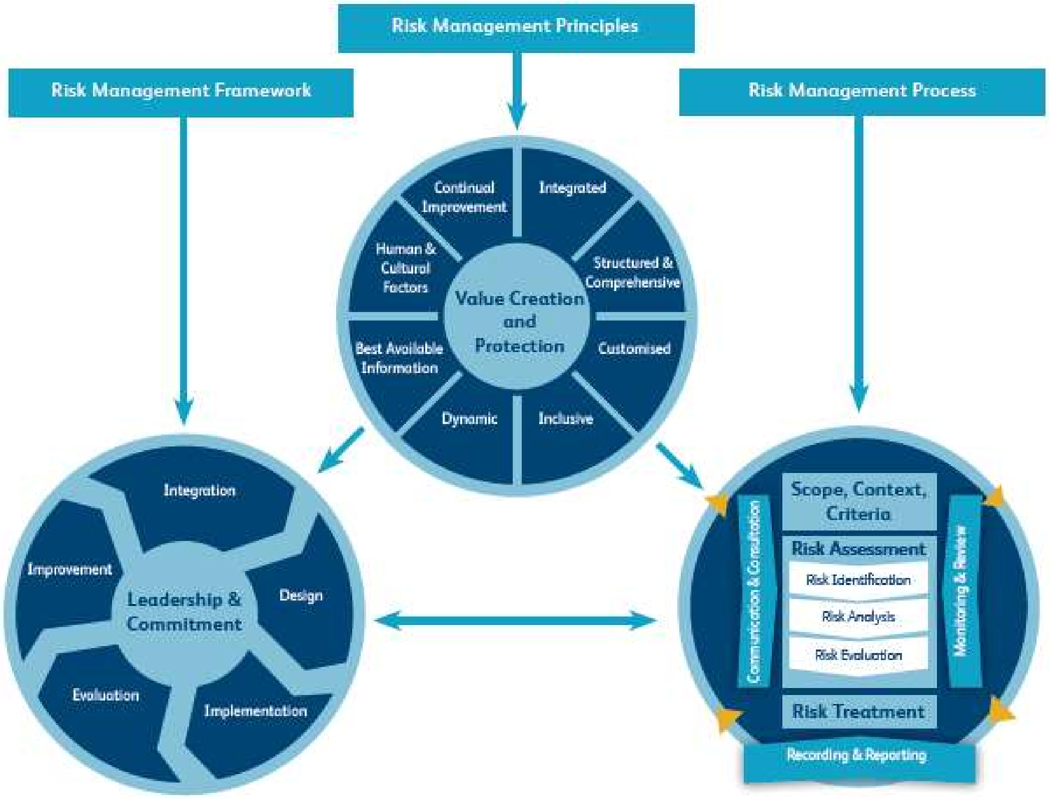
Outside - In approach, wherein the best global Risk Management practices will be benchmarked, and their approach embedded into the company's revised ERM framework.

Inside-Out Approach, wherein the internal company stakeholders would be required to provide insights into their respective functions in order to focus on specific risk areas which pose a threat to achievement of company's objectives. This approach would further be broken down into two parts:

- A **"Top-Down"** system, whose objectives are to distill insights and provide clarity on the **KEY RISKS** or the big, best shaping company performance, support risk-informed decisions at the Risk Management Committee levels, ensure a risk dialogue among the management team and enable proper risk oversight by the Board.

- A **"Bottom-Up"** system whose objectives are to ensure a comprehensive risk identification and prioritization of important risks, define and follow risk policies and processes that control daily decision making throughout the company and ensure a robust risk culture company-wide.

3.0 RISK MANAGEMENT PROCESS



(Source- ISO 31000)

Table 1 : Principles of Risk Management

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organization.
Aligned	Risk management activities need to be aligned with the other activities in the organization.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organization.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

Effective Risk Management process requires continuous and consistent assessment, mitigation, monitoring and reporting of risk issues across the full breadth of the enterprise. Essential to this process is a well- defined methodology for determining corporate direction and objectives. The risk management framework adopted by PLL is mapped as per the ISO Standard 31000: Risk Management – Principles and guidelines and is in-line with recommendations of The Committee of Sponsoring Organizations of the Tread way Commission ("COSO"). Hence, an enterprise wide and comprehensive view is being taken of risk management to address risks inherent to strategy, operations, finance and compliance and their resulting organizational impact.

The Risk Management process adopted by PLL has been tailored to the business processes of the organization. Broadly categorizing, the process consists of the following stages/steps:

- Establishing the Context
- Risk Assessment (identification, analysis, and evaluation)
- Risk Treatment (mitigation plan)
- Monitoring, review, and reporting
- Communication and consultation

3.1 Establishing the Context

"Establishing the Context" in the Risk Management process involves defining the organizational environment, including its objectives, stakeholders, and external factors. This step sets the foundation for effective risk management by providing a clear understanding of the internal and external context within which risks may arise.

Establishing the External Context

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

- The social and cultural, political, legal, regulatory, financial, technological, economic, natural, and competitive environment, whether international, national, regional, or local.
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with perceptions and values of external stakeholders
- Other international and national sanctions which might impact the company based on geo-political conditions.

Establishing the Internal Context

The risk management process should be aligned with the organization's culture, processes, structure, and strategy. Internal context is anything within the organization that can influence the way risks will be managed.

It is necessary to understand the internal context. This can include, but is not limited to:

- Governance, organizational structure, roles, and accountabilities.
- Policies, objectives, and the strategies that are in place to achieve them.
- Capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies).
- The relationships, perceptions, and values of internal stakeholders; the organization's culture.
- Information systems, information flows and decision-making processes (both formal and informal).
- Standards, guidelines, and models adopted by the organization.

3.2 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

3.2.1 Risk Identification

Risks are events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself. This stage involves identification of sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

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
- Cyber Risk
- Sustainability Risk
- Governance Risk
- Other Risk

A brief description of the factors to be considered for categorization of risks is detailed in Appendix 3.

3.2.2 Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk
- the trigger events that would lead to the occurrence of the risks.
- the positive and negative consequences of the risk
- the likelihood that those consequences can occur.

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be considered.

3.2.3 Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.
Decisions should take into account wider context of the risk and include consideration of the tolerance

of the risks borne by parties, other than the organization, which benefits from the risk. Decisions should be made in accordance with legal, regulatory, and other requirements.

[Refer Appendix 1 for details of the risk criteria, risk impact matrix and likelihood matrix]

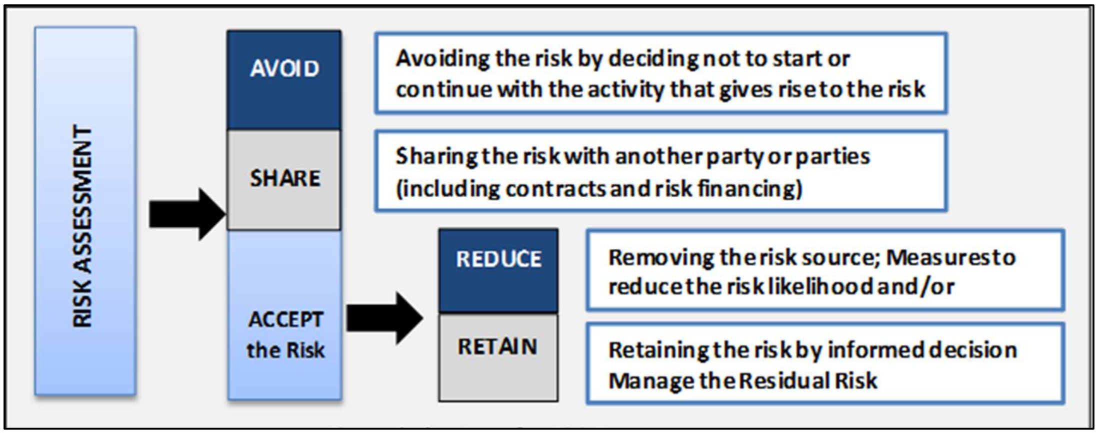
3.3 Risk Treatment

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment.
- Deciding whether residual risk levels are tolerable.
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:


RISK ASSESSMENT
AVOID
Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
SHARE
Sharing the risk with another party or parties (including contracts and risk financing)
ACCEPT the Risk
REDUCE
Removing the risk source; Measures to reduce the risk likelihood and/or
RETAIN
Retaining the risk by informed decision Manage the Residual Risk

(Source- ISO 31000)

1. **Avoidance (eliminate, withdraw from, or not become involved)**
   As the name suggests, risk avoidance implies not to start or continue with the activity that gives rise to the risk.
2. **Sharing (transfer - outsource or insure)**
   Sharing, with another party, the burden of loss or the benefit of gain, from a risk
3. **Reduction (optimize - mitigate)**
   Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.
4. **Retention (accept and budget)**
   Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default.

This includes risks that are so large or catastrophic that they either cannot be insured against, or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

3.4 Monitoring and review

All risks recorded in the risk register are reassessed, in order to ensure that risk management is effective and continues to support organizational performance. The monitoring and review mechanism is established by:

- Measuring risk management performance against the events, which are periodically reviewed for appropriateness.
- Periodically measuring progress against, and deviation from, the risk management plan
- Periodically reviewing whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context
- Reporting on risk, progress with the risk management plan and how well the risk management policy is being followed.
- Periodically reviewing the effectiveness of the risk management framework.
- Using structured scientific and analytical tools for this purpose.

3.5 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

4.0 RISK REPORTING

Reporting is an integral part of any process and critical from a monitoring perspective. Results of risk assessment needs to be reported to all relevant stake holders for review, inputs, and monitoring.

Approach towards implementation of ‘Risk Reporting’ at PLL is as follows:

A. The **Risk Owners** would be required to prepare department wise risk evaluation reports on a quarterly basis and submit to Risk Controllers for their review:

<u>Quarterly Risk Register Review Mechanism</u>

The Risk Owners shall submit their evaluation reports to Risk Controllers, and they (after risk owner’s responses) shall review the Risk Registers (impact and likelihood of existing risks) and identify any emerging/new risk and the existing control to mitigate that risk. They must ensure robustness of design and operating effectiveness of existing mitigating controls. If required, re–rate (existing risks)/rate (emerging risks) and prepare, implement action plan for risk treatment in situations where the existing controls are inadequate.

The quarterly Risk Register Review Report shall include:

- Risk rating movements, if any, along with reasons for changes in the impact and / or likelihood ratings
- New risks identified, if any, along with risk criteria ratings and mitigation plans
- Status of the implementation of mitigation plans and reasons for any delays or non-implementations
- Event / events materialized during the quarter that might have triggered any particular risk (not necessarily impacting the risk ratings) along with its mitigation measures.

B. Risk Controller, in consultation with risk owner, is required to review the risk register on a quarterly basis.

The Risk owner will be responsible for preparing and consolidating the report and the same shall be reviewed by Risk Controller and then subsequently by Risk Steering Committee (RSC).

C. The **Risk Management Department** headed by **Chief Risk Officer (CRO)** would be required, to prepare on a bi-annually basis, a report for the Risk Steering Committee detailing the following:

- List of applicable risks for the business, highlighting the new risks identified (if any) and the action taken w.r.t the existing and new risks.
- Prioritize list of risks highlighting the strategic and operational risks faced by PLL.
- Root causes and mitigation plans for the risks.
- Status of effectiveness of implementation of mitigation plans for the risks identified till date.

Movement in risk rating and new risks identified during each quarter should be duly apprised to RSC on quarterly basis.

Chief Risk Officer (CRO) and the Risk Management Team will be responsible for preparing and consolidating the report for the review, by the Risk Steering Committee.

D. The **Risk Steering Committee (RSC)** would be required to submit a report bi-annually, to the Risk Management Committee for its reviewal and approval.

Bi-Annual Risk Register Review Report

The Bi-annual risk register review report shall include:

- An overview of risk management process in place
- Observations on the status of risk management activities in the previous two quarters, (including as on date status for the immediately preceding quarter) along with any new risks identified and action taken w.r.t these risks.
- Status of effectiveness of implementation of mitigation plans for the Risks identified till date.
- High and Medium risks along with the events that materialized the risk during the period (if any) along with their mitigation plans.
- The risks having a severe impact, irrespective of their likelihood shall also be reported.
- Risk Management Team Structure (As per Section 5.0)

The Risk Steering Committee should meet at least one month prior to each RMC meeting.

Risk Culture Assessment:

A risk culture assessment shall be conducted once in every three years and the assessment report shall be presented to BOD for approval.

4.1 Risk Management Reporting Timelines

Level of Reporting	Stage of Risk	Timeline	Accountable To
BOD	Reporting to board on risk management in accordance with SEBI LODR, MCA, ISO 31000	Annually	Stakeholders
RMC	Review the finding of RSC	Bi-Annually	BOD / AC
RSC	Review/Moderation of approved risk along with mitigation plan and forward the findings of deliberation to RMC	Bi-Annually	RMC
CRO	Review approved risks and present the findings to Risk Steering Committee	Bi-Annually	RSC
Risk Controller	Approves risk along with action plan and forwards to Risk Management Department	Quarterly	CRO
Risk Owner	Risk owner completes the risk evaluation	Quarterly	Risk Controllers

- Endorsement of Director Incharge - Risk, would be required to present agenda to RMC.

- RSC to be held under overall guidance of Director Incharge Risk who shall be the Chairperson.

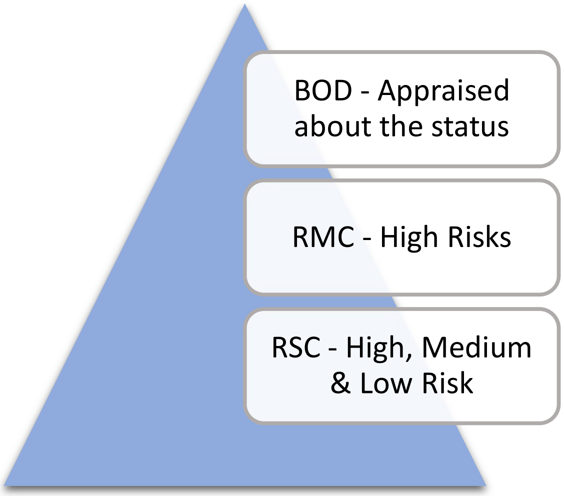
- RSC composition is as per the Risk organization structure as described below in section 5.0. For any deliberations/ requirements, Chief Risk Officer may invite concerned head/functional controllers.

- New risks or / and any change in the risk rating of existing risks during a quarter, must be apprised to RSC, on quarterly basis. CRO shall forward the report to the members of RSC.

- Risk Cards/ Register to be approved by RMC.

- Risk Controllers can be appointed as the member of RSC and shall report to CRO

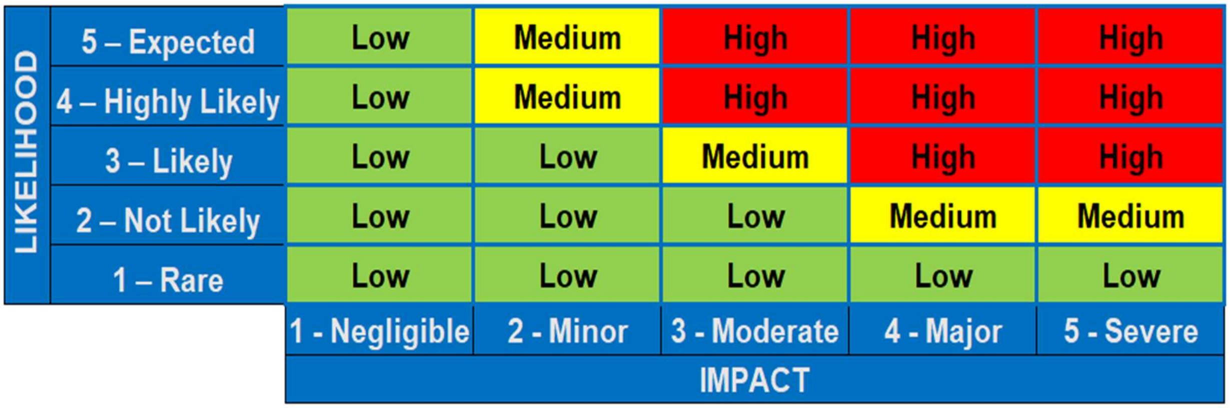
4.1 1 Risk Management Reporting


BOD - Appraised about the status
RMC - High Risks
RSC - High, Medium & Low Risk

4.1 2 Risk Rating

Level of Risk	Description	Quantified Rating (As per Impact and Likelihood)
HIGH	Senior management attention needed	>= 12
MEDIUM	Heads (HODs) attention required	>=8 and < 12
LOW	Can be managed by routine procedures	< 8

4.1.3 Risk Rating Heatmap



LIKELIHOOD	5 – Expected	Low	Medium	High	High	High
	4 – Highly Likely	Low	Medium	High	High	High
	3 – Likely	Low	Low	Medium	High	High
	2 – Not Likely	Low	Low	Low	Medium	Medium
	1 – Rare	Low	Low	Low	Low	Low
		1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Severe
		IMPACT				

4.2 Change Management

Risk Management action should also be undertaken to identify risks associated with changes to current business processes or changes in external environment. Change can be caused by internal events (i.e., internal reorganization or a major corporate initiative) or could be the result of external events (i.e., the impact of new environmental norms or change in regulatory requirement). The main difference between the two is the ability of the management to manage the risks that follow from these types of events.

A risk assessment should be considered if there is a major change in the way that business is undertaken within the business unit or if there is a major shift in the operating environment which could significantly impact the business unit.

Examples of circumstances where a risk assessment might prove useful, as it will help ensure that all risks are identified in relation to a specific issue or initiative might include:

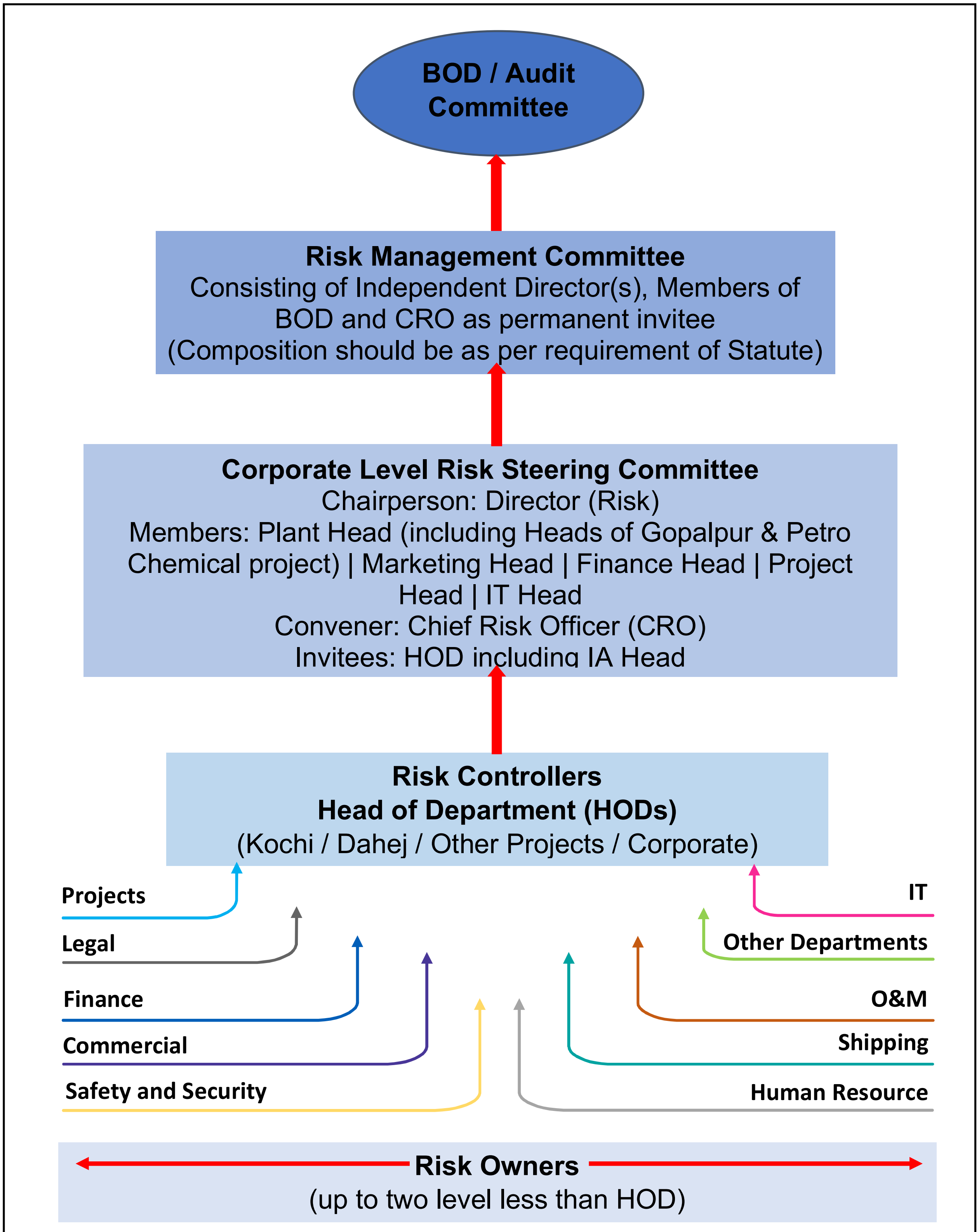
- Major changes within the regulatory environment (e.g., Changes in pricing mechanism)
- Major changes in the competitive landscape
- Merger/acquisition or divestment is proposed.
- Changes are proposed to internal policies and procedures.

Criteria for Addition of Risk: Department head should forward the new risks identified as and when to RSC for its approval. The same shall be approved by RMC in its subsequent meeting.

Criteria for Deletion of Risk: Deletion of risk shall be approved by RMC in its bi-annual meeting. The deleted risks shall be transferred to PLL’s Risk Repository.

Note: Risk identified / modified, approved by RSC shall be added to Risk Register. However, the same will be formally approved by RMC in its subsequent meeting. For deletion of any Risk, approval of RMC is mandatory.

5.0 RISK MANAGEMENT ORGANIZATION STRUCTURE



BOD / Audit Committee

Risk Management Committee
Consisting of Independent Director(s), Members of BOD and CRO as permanent invitee
(Composition should be as per requirement of Statute)

Corporate Level Risk Steering Committee
Chairperson: Director (Risk)
Members: Plant Head (including Heads of Gopalpur & Petro Chemical project) | Marketing Head | Finance Head | Project Head | IT Head
Convener: Chief Risk Officer (CRO)
Invitees: HOD including IA Head

Risk Controllers
Head of Department (HODs)
(Kochi / Dahej / Other Projects / Corporate)

Risk Owners
(up to two level less than HOD)

- Department heads to appoint Risk Owners – up to two level less than HOD.
- In cases where employee of required level / designation is unavailable for the formation of Risk Owners, exceptional approvals should be obtained from chairperson of RSC (Director Risk)
- Risk Controllers are to be appointed by each Director of their respective functions (not below Head of Department)

5.1 Roles and Responsibilities

Body	Constitution	Roles and Responsibilities
Board of Directors	Independent directors, Nominee directors and other Directors	• Approve Risk Management Policy including risk management approach and define risk appetite of the company. • Present Board Disclosures as mandated by SEBI (LODR) Regulations, on risk management to stock exchanges/ SEBI. • Review of RMC Charter from time to time to ensure it remains consistent and updated with the Committee's authority, objectives, and responsibilities. • Approve any amendment to the RMC Charter and policy
Risk Management Committee (RMC)	➢ Independent Director(s) ➢ Members of Board of Directors ➢ CRO shall be a permanent invitee. ➢ Composition shall be in accordance with the requirements of Companies Act and SEBI LODR or any other applicable act / rules	• Review and approve RSC risk assessment bi-annually and shall review the exception reports along with effectiveness of the mitigation plans. • To monitor significant changes in the risk profile, including changes/events outside the risk appetite of the company. • To provide leadership and direction to the company on the Risk Management framework. • 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), information, cyber security risks, Business Continuity Plan (BCP) or any other risks as may be determined by the Committee. • To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems. • 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. • To keep the board of directors informed about the nature and content of its discussions, recommendations, and actions to be taken. • To submit reports as desired by the Audit Committee/Board of Directors • Deliberate over modifications, additions and deletions of risks and their mitigation plans. • Performance of duties and assumption of responsibilities as per RMC charter • Any other matter as decided by the Board of Directors or as specified under the provisions of Companies Act, 2013 and SEBI (LODR) Regulations, as amended from time to time.

		• The appointment, removal, and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee. • Reviews and approves the enterprise risk register bi-annually. Reviews RSC findings resulting out of moderation of quarterly risk evaluation report. • 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. • To submit Risk Culture Assessment to Board of Directors for its approval
Risk Steering Committee (RSC)	➢ **Chairperson**: Director Incharge Risk i.e. Director Technical ➢ **Members**: Following Heads of Departments (HoD) at corporate office: • Finance & Account • Marketing • Projects • IT • Plant heads post commissioning of Petro-chemical plant at Dahej and Gopalpur LNG Terminal shall also be members of RSC. ➢ **Convener:** Chief Risk Officer (CRO) ➢ **Invitees**: HODs including IA Head	• Preparation and Update of the Corporate Level Risk Register and Bi-annual reports for RMC. • Monitor risks, risk response, performance evaluation and continuous improvement of risk management function. • Providing assurance to the management for operating effectively. • Reviewing mitigating measures are in place and assessing their adequacy. • Ensuring the implementation of risk mitigation plans through appropriate direction to the concerned executing agencies. • Examining observations and management action plan of audit finding of Enterprise Risk Management. • Monitoring the environment within which the risk exists to identify issues which may affect its impact on the company or the likelihood of its arising. • Approval of new risk for presenting to RMC
Risk Management Department headed by CRO	➢ Works closely with Director Incharge Risk, and the Board. ➢ CRO to be the convener of RSC and will be a permanent invitee to RMC. ➢ CRO will have functional and administrative reporting to Director Incharge Risk.	• 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 collaborating with managers to establish control activities and recommending corrective action where needed. • Collate updates/ changes in the risk register as received from respective process owners (post approval) • Present Risk Register to the RMC periodically • Will present the quarterly risk management review report to the Corporate Level Risk Steering Committee (RSC). • The Team will be responsible for coordinating with respective Risk coordinators, Risk owners, Risk Controllers and consolidating the quarterly risk register review reports.

		• Implement appropriate risk reporting to the Board and senior management. • Facilitating enterprise-wide risk assessments, developing of risk mitigation strategies where required, and monitoring risks across the organization. • Assist management with integrating risk management with the strategy development process. • Assist the Board and RMC to develop and communicate risk management policies. • Risk Repository shall be reviewed by CRO every 6 months.
Risk Controllers	Risk Controller to be appointed by Head of Department for their respective functions covered under their ambit	• Guiding and monitoring application of enterprise risk management within their spheres of responsibility • 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 • Presenting status of risks to the Chief Risk Officer (CRO) on quarterly basis • Review and approve reports submitted by the Risk owners. • Review of the Risk Register on quarterly basis. • Coordinate the various Risks owners to identify, analyze and manage risks. • Developing risk response processes. • Review the implementation of risk mitigation plans. • Endorsing/Sponsoring modification in risk, addition of risk, addition of mitigating control activity to RSC / CRO / Director
Risk Owners	Department heads to appoint Risk Owners – up to two level less than HOD	• Compliance with risk policy requirements and management directives • Exercise reasonable care to prevent loss, to maximize opportunity and to ensure that the operations, reputation, and assets are not adversely affected. • Keeping the risk registers and related action plans updated. • Consolidating the quarterly and annual risk register review reports and timely reporting to the Risk Management Department. • Educating employees dealing with key activities in their unit of the risk management process. • Implementation of risk mitigation plan in coordination with Department Head. • Reviewing and discussing significant risk issues and ensuring horizontal collaboration in the development of mitigation strategies and the establishment of corporate priorities in resource allocation. • Identification of new risks/ events of recurring nature which may lead to risk within respective business function(s) and reporting new risks or failures of existing control measures with remedial action to Risk Controller. • Ensuring Management Action Plans developed, in response to audit and evaluation recommendations are adequately addressing the risk. • Responsible for submission of quarterly risk review reports to Risk Controllers

5.1.1 Risk Steering Committee

Apart from the responsibilities mentioned in Table 5.1, key responsibilities of the Committee also include the following:

- Approval of new risk will be conducted by RSC and subsequently forwarded for ratification from Risk Management Committee.
- Monitoring the Internal and/or external environment within which the risk exists to identify issues which may affect its impact or the likelihood of its occurrence on the company.
- Reviewing risk response processes and assessing adequacy of responses for the risks identified through the risk management framework.

Reporting:

- Reviews and approves risk response plans, identified risks and emerging changes.
- Reports to the Risk Management Committee bi-annually.
- Examining observations and management action plan of audit finding of Enterprise Risk Management

5.1.2 Chief Risk Officer and the Risk Management Department

The Chief Risk Officer (CRO) plays a pivotal role in the oversight and execution of a company's risk management function. Working closely with the Director Incharge Risk, the CRO is responsible for developing and implementing risk assessment policies, monitoring strategies, and implementing risk management capabilities. The CRO's ultimate objective is to help the Board and executive management to determine the risk-reward tradeoffs in the business and bring unfettered transparency into the risk profile of the business.

The CRO should be adequately supported by a team of experienced risk personnel along with technical expertise personnel, collectively known as Risk Management Department. The team works closely with other departments to identify risks and then evaluate and negotiate risk response plans based on cost-benefit analysis. As the ERM champion, the CRO facilitates the execution of risk management processes and infrastructure as a key enabler to achieving the business objectives of the organization.

Apart from the responsibilities covered in Table 5.1, following are other key responsibilities of the CRO and Risk Management Team:

- Assist the board/RMC and senior management to establish and communicate the organization's ERM objectives and direction.
- The CRO will be an officer of adequate experience to be able to adeptly coordinate with senior level PLL personnel with proven experience in handling complex assignments. A Chief Risk Officer should possess the following qualities:
  - ➢ Blend of specialized statistical, actuarial, financial, and economic modelling skills together with a dash of old-fashioned business nous.
  - ➢ Should be able to assemble and develop the requisite skill sets and encourages a creative interaction between risk management specialists and the organization's executive team to produce insightful and reliable conclusions.
  - ➢ Should possess sound overall business knowledge, strong analytical skills, and ability to place technical risk issues into broader business contexts.
  - ➢ Should be able to inject an element of objectivity and balance into the deliberations. He or she should be conscious of the limitations of current risk management practices, avoid offering certainty where none exists and keep discussions grounded in reality.
  - ➢ Should be able to assist the board and management to stress test their risk register and consider contingent risks.

Adequate training and exposure will be imparted to the CRO and his team by third party or in-house experts on the same. An Orientation Pack/ training needs should be identified for CRO. A ‘Risk Management Training’ should also be imparted to all the new joiners at the time of joining.

5.1.3 Risk Controller

The Functional Risk Controllers will set the risk management procedures and coordinate with Risk owners in reporting risks to the CRO by following the standard operating procedure. The roles and responsibilities are already covered in Table 5.1

Reporting:

- Reviews and approves risk response plans, identified risks and emerging changes.
- Receipt of quarterly/ event driven status updates and ad-hoc deep dive materials, provided by Risk Owners.
- Reports to the RSC on an event-driven frequency.

5.1.4 Risk Owner

Risk owners at a plant/unit/department in consultation with Risk Controllers will assess the risk by determining its probability of occurrence and its impact with an objective of reporting risks to the Risk Controller. The roles and responsibilities are covered in Table 5.1.

Reporting:

- Provides quarterly status updates and reports the same to their associated Risk Controller.

APPENDIX

APPENDIX 1: RISK RATING CRITERIA

The Risk Rating Criteria, a key element of the risk management framework seeks to establish the standard for prioritizing the risk based on the assessment of the following:

- **Impact** of the risk on the stated objectives and goals: The degree of consequences to the organization should the event occur.
- **Likelihood** of occurrence of the risk: The likelihood of the event occurring expressed as an indicative annual frequency.

The risk rating for a risk that falls in two or more likelihood / impact parameters, should be treated among the one with the highest likelihood / impact.

Likelihood Matrix

	Likelihood Score				
Likelihood Criteria	**1 – Rare**	**2 – Not Likely**	**3 – Likely**	**4 – Highly Likely**	**5 – Expected**
Occurrence in future	Not likely, almost impossible to occur within two to five years (from now)	May occur once or twice between two to five years (from now).	Possible, may arise once or twice within the next year.	High, may arise in several months (not in all months) within the next year	Very high, will be almost a routine instance every month (greater than or equal to 12 instances) within the next year.
Occurrence in past	Similar instances have never occurred in the past in the industry	Though not routinely but there have been instances in the last 2 to 5 years within PLL or outside	There have been one or two similar instances in the past year within PLL or outside	Similar instances have occurred in several months (not in all months) in the past year within PLL or outside.	Similar instances have commonly occurred every month (greater than or equal to 12 instances) in the past year.
Probability (In %)	<= 5%	>5% and <= 10%	>10 and <= 50%	>50 and <= 80%	>80%
Note: The 'Year' to be counted from the immediate day following the quarter in which RMC meeting is conducted					

Impact Matrix

	Impact Score				
Description	**1 - Negligible**	**2 - Minor**	**3 - Moderate**	**4 - Major**	**5 - Severe**
Reduction in capacity utilization	Less than 0.5%	0.5 to 1%	1 to 2%	2 to 3%	Greater than 3%
Impact on annual profitability (PBDIT)	Less than 0.5%	0.5 to 1%	1 to 2%	2 to 3%	Greater than 3%
Financial Impact	Less than INR 5 Cr	> INR 5 Cr to 10 Cr	> INR 10 Cr to 50 Cr	> INR 50 Cr to 100 Cr	> INR 100 Cr
Community/Social, Reputation, Media	Minor, medium- term social impacts on local population; mostly repairable. Minor, adverse local public, and media attention	Ongoing social issues; significant damage to items of cultural significance. Attention from media; heightened concern by local community	Ongoing serious social issues; significant damage to structures or items of cultural significance. Criticism by national government.	Ongoing serious social issues; significant damage to structures or items of cultural significance. Significant adverse national media or public or national government attention	Ongoing serious social issues; significant damage to structures or items of cultural significance. Serious public or media outcry; international coverage
Delay in completion of projects from schedule timelines	Delay up to 5% of project duration	Delay from 5 to 7.5% of project duration	Delay from 7.5 to 10% of project duration	Delay from 10 to 15% of project duration	Delay of more than 15% of project duration
Interruption in Plant Operations (days lost on due to disruptions/interruptions)	< 6 hours	6-12 hours	12-24 hours	1-2 days	> 2 days, due to closure of manufacturing facility
Health, Safety, Security / Property damage: Loss of life and/or property due to accidents/ thefts	Physical discomfort / damage up to 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

	Impact Score				
Description	**1 - Negligible**	**2 - Minor**	**3 - Moderate**	**4 - Major**	**5 - Severe**
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 localized 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 imprisonment of director(s)
Interventions: Level of escalations	Department Head	Department VP/ President	Director	MD	BOD
Loss of Key Alliances (Key alliances means vendor /customer or 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%

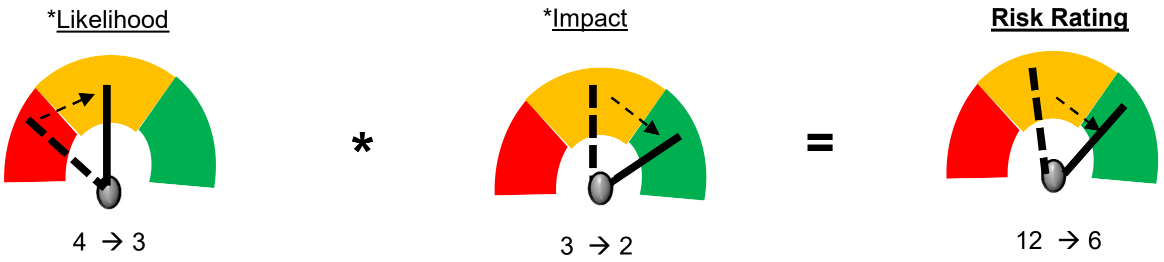
Movement in Risk Rating

Scoring Map – Inherent Risk

Risk ○

LIKELIHOOD	5 – Expected	Low	Medium	High	High	High ○
	4 – Highly Likely	Low	Medium	High	High	High
	3 – Likely	Low	Low	Medium ○	High	High
	2 – Not Likely	Low	Low ○	Low	Medium	Medium
	1 – Rare	Low	Low	Low	Low	Low
Risk = Impact * Likelihood		1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Severe
		IMPACT				

Any change in risk rating of risk defined in risk register requires approval of the RSC and RMC. Changes in risk can happen due to changes in impact and likelihood of risk. Mitigating control activities would result in changes to likelihood and impact:



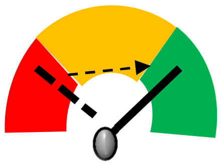
Post introduction of mitigating control Likelihood rating changes from 4 to 3

Post introduction of mitigating control Impact rating changes from 3 to 2

Post introduction of mitigating control Risk rating changes from 12 to 6

Inherent and Residual Risk

- **Inherent risk** represents the amount of risk that exists in the absence of controls. Inherent Risk is typically defined as the level of risk in place in order to achieve an entity's objectives and before actions are taken to alter the risk's impact or likelihood.
- **Residual risk** is the amount of risk that remains after controls are accounted for. Residual Risk is the remaining level of risk following the development and implementation of the entity's response.



Inherent Risk 16 (4*4)

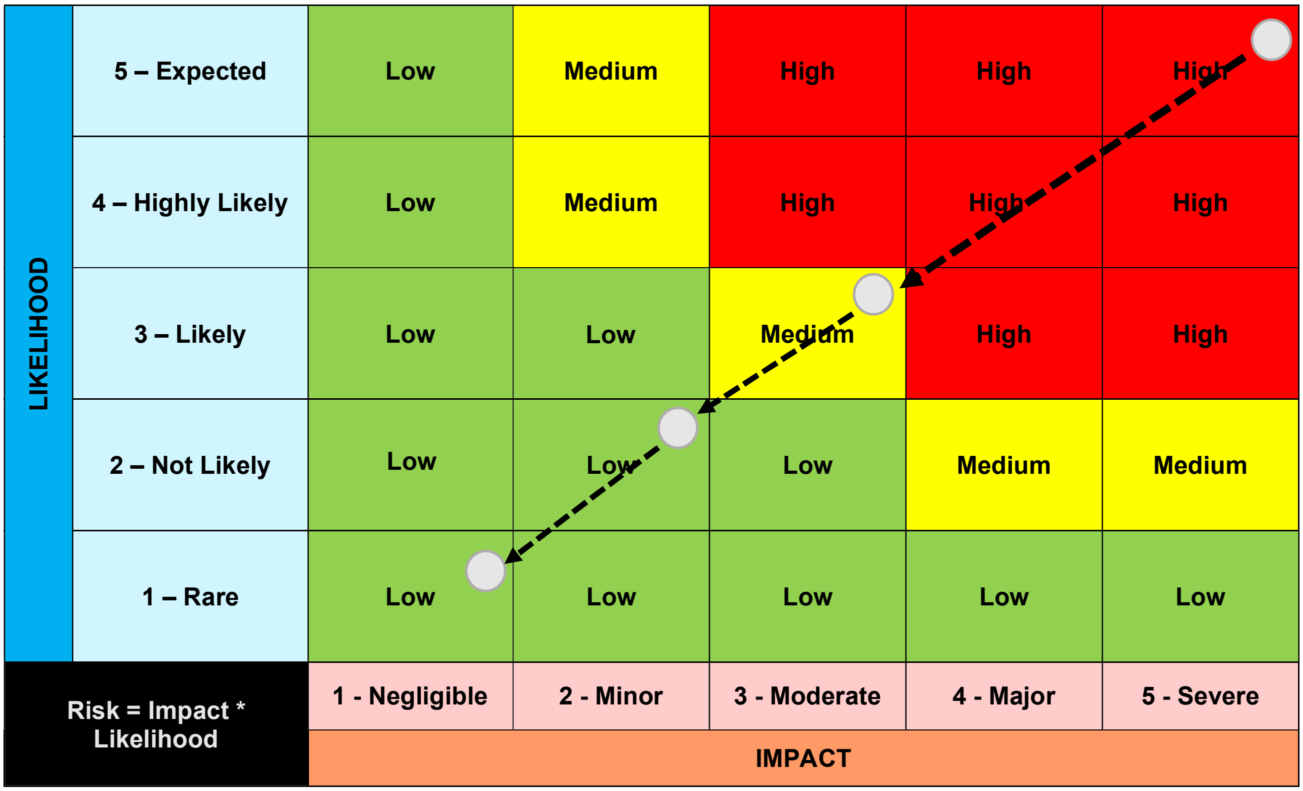
Residual risk is 6 (3*2)

In the above figure, if the inherent risk rating basis impact (4) and likelihood (4) was 16 before a mitigating control in place, the same risk has a residual risk rating of 6, impact (3) and likelihood (2) post introduction of a control activity.

If any new mitigation or control will be mapped against the risk, then subsequently Risk Management Committee will be informed on periodic basis about the movement of risk from inherent to residual rating and the above methodology can be used to show the change in risk rating to Risk Management Committee (RMC).

Scoring Map – Residual Risk

Risk ○



LIKELIHOOD	5 – Expected	Low	Medium	High	High	High
	4 – Highly Likely	Low	Medium	High	High	High
	3 – Likely	Low	Low	Medium	High	High
	2 – Not Likely	Low	Low	Low	Medium	Medium
	1 – Rare	Low	Low	Low	Low	Low
Risk = Impact * Likelihood		1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Severe
		IMPACT				

APPENDIX 2: RISK REPORTING FORMAT

Quarterly Risk Register Review Report (Illustrative)

<table>
<tr><th colspan="6">Quarterly Risk Register Review Report Function <To be updated&gt;</th></tr>
<tr><th colspan="6">Department: XXX</th></tr>
<tr><th>Function</th><th>Risk Description</th><th>Risk Score</th><th colspan="2">Proposed Risk Mitigation Plan</th><th>Status of implementation of Risk Mitigation Plan</th></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="6"><b>Risk Owner: <Name&gt;</b></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td></tr>
<tr><td colspan="2">(Signature)</td><td colspan="3">(Designation)</td><td>(Date of approval)</td></tr>
<tr><td colspan="6">Comments:</td></tr>
<tr><td colspan="6"><b>Approved by Risk Controller: <Name&gt;</b></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td><td></td></tr>
<tr><td colspan="2">(Signature)</td><td colspan="3">(Designation)</td><td>(Date of approval)</td></tr>
<tr><td colspan="6">Comments:</td></tr>
<tr><td colspan="6"><i>Presented to the Office of Chief Risk Officer</i></td></tr>
</table>

- Risk Review report (Risk Register) shall be presented to RMC by CRO after reviewal of RSC.

APPENDIX 3: FACTORS TO BE CONSIDERED FOR RISK CATEGORIZATION

Categories	Factors
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?
Cybersecurity Risk	• How does the organization respond to cyberattacks? • How does the organization stay informed about evolving cybersecurity threats and adapt its defenses accordingly?
ESG Risks	• Is the organization able to manage its environmental footprint? • How does the organization monitor and manage its social impact on employees, communities, and stakeholders?
Sectoral Risk	• How well does the organization understand and monitor the evolving landscape of the LNG sector, including trends in geopolitical scenarios, energy transition, and technology? • How does the organization respond to major disruptions or unforeseen events impacting the LNG sector?
Health and Safety	• Are current safety protocols and procedures adequate to prevent accidents, injuries, and fatalities across all operations? • Does the organization have a strong safety culture that emphasizes continuous improvement, employee involvement, and reporting of near-misses and incidents?

Annexure 2:

BUSINESS CONTINUITY POLICY

BUSINESS CONTINUITY POLICY

Terms and Definition

BCMS	Business Continuity Management System
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
RA	Risk Assessment
RMC	Risk Management Committee
Activity	Process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more processes and services
Audit	Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
Business Continuity Programme	Ongoing management and governance process supported by Senior Management and appropriately resourced to implement and maintain business continuity management
Competence	Ability to apply knowledge and skills to achieve intended results
Conformity	Fulfilment of a requirement
Continual Improvement	Recurring activity to enhance performance
Correction	Action to eliminate a detected nonconformity
Corrective Action (CA)	Action to eliminate the cause of a nonconformity and to prevent recurrence
Effectiveness	Extent to which planned activities are realized and planned results achieved
Event	Occurrence or change of a particular set of circumstances
Exercise	Process to train for, assess, practice, and improve performance in an organization
Incident	Situation that might be, or could lead to, a disruption, loss, emergency, or crisis
Infrastructure	System of facilities, equipment and services needed for the operation of an organization
Interested Party (Stakeholder)	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Internal Audit	Audit conducted by, or on behalf of, the organization itself for management review and other internal purposes, and which might form the basis for an organization's self-declaration of conformity
Invocation	Act of declaring that an organization's business continuity arrangements need to be put into effect in order to continue delivery of key functions or services
Management System	Set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives
Maximum Acceptable Outage (MAO)	Time it would take for adverse impacts, which might arise as a result of not providing a function / Service or performing an activity, to become unacceptable
Measurement	Process to determine a value
Minimum Business Continuity Objective (MBCO)	Minimum level of services/operations that is acceptable to the organization to achieve its business Objectives during a disruption
Monitoring	Determining the status of a system, a process, or an activity
Nonconformity	Non-fulfilment of a requirement
Objective	Result to be achieved
Recovery Time Objective (RTO)	Period of time following an incident within which • Processes must be resumed, or • Activity must be resumed, or • Resources must be recovered

Table 1: Key terminologies

1. Introduction

Petronet LNG Limited (hereafter may be referred to as “the company” or “the organization” or “PLL”) is one of the fastest growing world-class Public Limited Company in the Indian energy sector. It has set up the country's first LNG receiving and regasification terminal at Dahej, Gujarat with present nominal capacity of 17.5 MMTPA and another terminal at Kochi, Kerala having a nominal capacity of 5 MMTPA. The company is also exploring suitable opportunities within and outside India to expand its business presence. The organization is committed to its customers, employees and interested parties to ensure necessary efforts are made to safeguard the life and safety of personnel deployed within its premises and all the applicable requirements are met, critical client services are resumed at the earliest in the event of any untoward scenarios.

It recognizes that it is necessary for it to develop strategic and tactical capability to plan and respond to incidents and disruptions in order to continue business operations at an acceptable level of downtime. In addition to providing safety of employees, this policy provides guidance for the resumption and recovery of time sensitive business operations in accordance with pre-established timeframes as well as ensuring that adequate plans are in place for the less critical business operations.

Refer Terms and Definitions for further information.

2. Context of the Organization

The organization has its registered and corporate offices in New Delhi, India, and employs approximately 558 people across its corporate office and its two plant locations in Dahej, Gujarat, and Kochi, Kerala, to service its clients.

The business-critical processes involve import, storage, and regasification of LNG, maintaining terminal operations and continuous supply of natural gas to customers via pipelines or trucks. The service delivery is enabled by PLL's core infrastructure and support services being delivered from its two plants i.e., Dahej and Kochi making them the mainstay of BCMS at PLL.

2.1 BCM Policy Scope and Exclusions

The Business Continuity Policy outlined in this document is applicable to all departments of PLL across its Head Office, Dahej and Kochi Terminals

The BCM policy shall be adhered by all the personnel who have access to the in-scope PLL locations/facilities, services, premises, information, networks, and assets. The main purpose of the Business Continuity Management policy is to inform interested parties i.e., employees, contractors, and other authorized users of their obligatory requirements for ensuring business continuity at PLL. PLL shall ensure that the Business Continuity Policy is updated once in two years to accommodate changes in the existing framework and if there are any new additions to the scope of BCMS.

2.2 Understanding the organization and requirement for Business Continuity Policy

PLL recognizes the potential financial, operational, reputational, legal, contractual, regulatory and stakeholder support related risks associated with business interruptions and the importance of maintaining viable capability to continue business operations with minimum impact in the event of a disaster or crisis.

PLL recognizes the following as primary reasons for instituting Business Continuity Management Policy:

- To develop appropriate measures to safeguard employee interests in the event of a disaster.
- To have a streamlined and unified crisis response and communication process in the event of a disaster.
- To demonstrate business resilience and enhance customer confidence.
- To minimize potential adverse regulatory and financial impact due to failure in service delivery and stipulated turnaround times.
- To minimize the impact to reputation and public image.

2.2.1 Internal and External Factors

Internal Factors

- Failure to continue critical processes of the organization.
- Compliance to regulatory requirements.
- Maintaining reputation of having reliable operations even in case of disruptions.
- Redundant processes, competencies, and skills.

External Factors

- Vulnerable single sources of critical suppliers/vendors
- Geo-political issues such as regional or local political instability, strikes, etc.
- Market conditions such as competitive landscape and emerging technologies.
-

- Expectations of customers and interested parties with regards to response to disruptions due to severe natural calamities, disruption to utilities, transportation, strikes, pandemic, illness, significant security breaches and major public events.

2.2.2 Understanding the Needs & Expectations of Interested Parties

S.No.	Interested Party	BCMS Requirement
1.	Employees	Appropriate measures to safeguard employee interests in the event of a disaster.
2.	Business Partners and Stakeholders	PLL shall endeavour to lower business risks arising from serious incidents and demonstrate business resilience, safeguard reputation and public image.
3.	Customers	PLL shall ensure seamless and uninterrupted delivery of its services and maintaining high service availability to uphold customer trust and loyalty.
4.	Suppliers	PLL shall lower business risks arising from serious incidents at vendor's end.
5.	Public Authorities	PLL shall demonstrate business resilience and regulatory compliance.
6.	Legal & Regulatory Bodies	PLL shall minimize potential adverse regulatory and financial impact due to failure in service delivery at agreed timelines.

Table 3: Interested Parties and their requirements.

2.2.3 Legal and regulatory requirements

Compliance to Legal, Regulatory, Contractual and Statutory requirements is critical to the organization's continuity of operations. Therefore, the organization shall establish a procedure to identify and ensure compliance with applicable legal, statutory, and regulatory requirements with regard to the continuity of its operations. The requirements will be documented, kept up-to-date and communicated to all impacted interested parties, if required.

2. BCMS Framework

PLL BCMS applies the standard of Plan-Do- Check- Act (PDCA) model for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving the effectiveness of BCMS. The below image illustrates how a BCMS takes inputs from interested parties and requirements for continuity management and through the necessary actions, process, procedures to achieve business continuity outcomes.

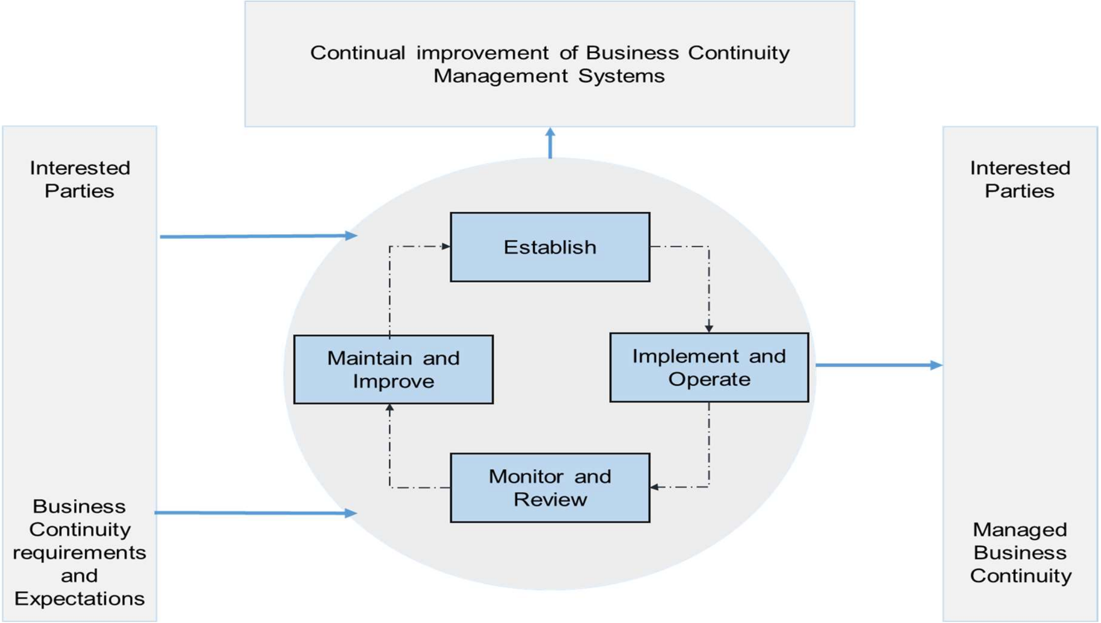

Continual improvement of Business Continuity Management Systems
Interested Parties
Business Continuity requirements and Expectations
Establish
Implement and Operate
Monitor and Review
Maintain and Improve
Interested Parties
Managed Business Continuity

Figure 1: BCMS PDCA Lifecycle

Plan	Establish Business Continuity Policy, objectives, targets, controls, processes, and procedures relevant to managing risk and improving business continuity to deliver results in accordance with an organization's overall policies and objectives
Do	Implement and operate the Business Continuity Policy, controls, processes, and procedures.
Check	Monitor and review performance against business continuity objectives and policy, report the results to management, and determine and authorize actions for remediation and improvement.
Act	Maintain and improve the BCMS by taking preventive and corrective actions, based on the results of management review, and re-appraising the scope of the BCMS and business continuity objectives and policy.

Table 4: PDCA Matrix

3. Business Continuity Program Objectives

This BCMS policy articulates the commitment of PLL to establish and sustain a robust Business Continuity Planning framework. The objective is to ensure the uninterrupted delivery of all critical and vital services, safeguarding the interests of our customers and stakeholders in the face of unforeseen disruptions. PLL is dedicated to implement BCM practices that align with industry standards like ISO 22301:2019.

The organization's core BCM objectives have been identified as:

- Ensuring safety of people/employees, infrastructure, critical functions/process, information and other assets through appropriate safety and security strategies during an incident.
- Proactively identify potential risks of disruption along with appropriate strategies and actions to ensure the availability of critical services during any disruption.
- Ensuring continuity of identified critical business functions/processes within the stipulated recovery timeframe with minimal impact due to disruption.
-

- Ensuring that Business Continuity requirements are assessed, resources allocated, recovery and continuity strategy are updated, and Business Continuity Plans (BCPs) are comprehensive, complete, and tested at regular intervals.
- Ensure effective communication with internal and external emergency responders, employees, customers, investors, media, and relevant interested parties during an incident or disruption.
- Continuously monitor and improve the BCMS to ensure alignment with overall business objective.
- Timely detection of incidents/disruption and minimizing impact through effective crisis response, and business continuity plans.
- Integrate business continuity management system requirements with the requirements of other existing PLL management systems/policies.
- Embed a holistic BCM culture across our company to make our employees and third parties (such as outsourced service providers, contractors, etc.) understand their roles and responsibilities towards the organization's business continuity requirements through awareness, training, and contractual agreements.

To achieve business continuity objectives, the management shall determine what actions need to be planned, the resources required to support these actions, when will these actions be completed, who will be responsible and how the results of these actions will be evaluated. The organization considers People’s safety as its top priority and other business continuity objective priorities will be based on decisions made by the management. The BCM objectives are consistent with the contractual, statutory, and other applicable requirements. The business continuity objectives would ensure minimum levels of key services in order to achieve the organization’s business objectives during a disruption. PLL senior management shall ensure these business continuity objectives are implemented and communicated within the organization. The management shall also ensure business continuity objectives are established at all identified critical functions and processes.

4. About the Policy

The Business continuity management policy is based on the organization’s core business continuity objectives that forms the basis of driving business continuity at both corporate as well as at terminal/ site level and is aligned with the company’s business objectives.

The Policy shall be approved by the PLL’s Board of Directors. The Policy shall be reviewed and approved at least once in two years. Further it may be reviewed in case of changes to strategic objectives, change in business environment, operating environment which may have an impact to Business Continuity posture as deemed necessary.

This BCM Policy shall be communicated to all employees including staff of PLL and other interested parties (as per requirement) by publishing in an intranet portal.

The policy will help to put in place a management system that provides a framework for setting business continuity objectives, identifies potential threats to the organization and evaluates the impacts to its business that these threats, if realized, may cause, and which will provide a framework for building resilience. The system will also allow the organization to develop effective responses that meet the needs and requirements of its interested parties, reputation, and brand. Further, this system will allow the organization to manage the overall programme through training, exercises, audits, and reviews to ensure that the business continuity plans stay current and up to date.

5. Policy Statement

PLL shall implement and sustain:

A Business Continuity Management System that is appropriate for the purpose of the organization to ensure Safety of its people, Continuity of critical business operations and Delivery of products and services (limited to people, technology, infrastructure and facility) within the organization while abiding to legal, contractual and regulatory obligations and also acts as a framework for identifying applicable requirements, setting objectives for business continuity and achieving them, while evaluating performance and continually improving them. The Business Continuity Management System has been designed using the international standard ISO 22301: 2019 (E) – Security and resilience — Business continuity management systems — Requirements.

6. Leadership

Management's commitment is imperative for the success of the BCMS program at the organization. In order to achieve the intended outcome of the BCMS, senior management and management at all levels will clearly demonstrate their support and commitment for the BCMS by

- Ensuring that the business continuity policy and business continuity objectives are established and are compatible with the strategic direction of the organization
- Ensuring the integration of the BCMS requirements into the organization's business processes;
- Ensuring that the resources needed for the BCMS are available and appropriate roles and responsibilities are defined;
- Communicating the importance of effective business continuity and of conforming to the BCMS requirements;
- Ensuring that the BCMS achieves its intended outcomes;
- Directing and supporting persons to contribute to the effectiveness of the BCMS;
- Promoting continual improvement through the BCM program;
- Supporting other relevant managerial roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.

Further, the PLL Management shall appoint one or more persons and assign the responsibility and accountability for implementing and maintaining the BCMS at PLL.

7. Changes to Business Continuity Management System

The organization shall identify the requirements for changes to BCMS and these shall be implemented in a planned manner following organization's change management process, considering:

- Purpose and consequences of the changes
- Effects on the BCMS's integrity
- Availability of resources
- Impact to current responsibilities and authorities that are defined for BCMS

8. Actions to address risk and opportunities

PLL shall ensure that risk and opportunities identified with respect to its Business Continuity Management System (BCMS) are addressed. The organization shall therefore plan actions to address risks and opportunities as well as integrate these actions to BCMS processes and evaluate their effectiveness.

9. Support

10.1 Resources

The resources that are required to establish, implement, operate, and maintain and continually improve the BCMS shall be determined and provided by the top management. The types of resources considered will include, but not be limited to human resources, information & data, building, work environment and associated utilities, facilities, equipment and consumables, information & communication technology systems, transportation, finance, and third-party requirements.

10.2 Competence

PLL' s management shall ensure that the resources who are assigned to perform BCM roles meet the competence levels with respect to Education, Training, and work experience, as will be determined in the Learning & Development SOPs from time to time.

It should be ensured that appropriate actions are taken to acquire necessary competence, where applicable, and the effectiveness of the actions taken evaluated periodically. Appropriate documentation, including records of education, training, skills, experience, and qualifications shall be maintained as evidence of competence.

10.3 Education, Awareness and Training Program

The organization appreciates the importance of employee's awareness on Business Continuity arrangements and procedures. In order to ensure that employees are educated, trained and are aware of BCM arrangements in the organization, an 'Education, Awareness and Training' Program shall be periodically implemented in PLL.

10.4 Communication

The BCM Policy shall be communicated to all employees (including permanent staff and contractual employees), third parties and other interested parties (as per requirement) by publishing on an intranet portal.

PLL shall determine the internal and external communications relevant to the BCMS by defining the following key elements: what information to communicate, the timing of communication, the target audience, the communication method, and the designated communicator. This structured approach ensures that all stakeholders are informed effectively and efficiently, facilitating seamless business continuity, and minimizing impact of disruptions.

10.5 Control of Documented Information

The purpose of controlling documented information is to ensure that the organization creates, maintains, and protects documents in a manner that is appropriate and sufficient to implement and maintain the BCMS framework. Documented information of BCMS should be controlled so as to ensure they are available when needed and adequately protected from disclosure, alteration, and deletion.

Documented information of external origin that are necessary for the planning and operation of the BCMS should also be identified and controlled.

10. BCM Organization

The organization shall have a defined governance and organization structure for BCMS with representation from senior management, head of functions and a dedicated business continuity team to drive business continuity program across the organization. BCM organization structure will ensure that the Business Continuity Management System is implemented, operated, and continually improved to meet the business continuity objectives of the organization with competent resources, clearly defined roles, responsibilities, and predefined authority have been appointed. The PLL BCMS Organization for implementation and maintenance of BCMS consists of the following:

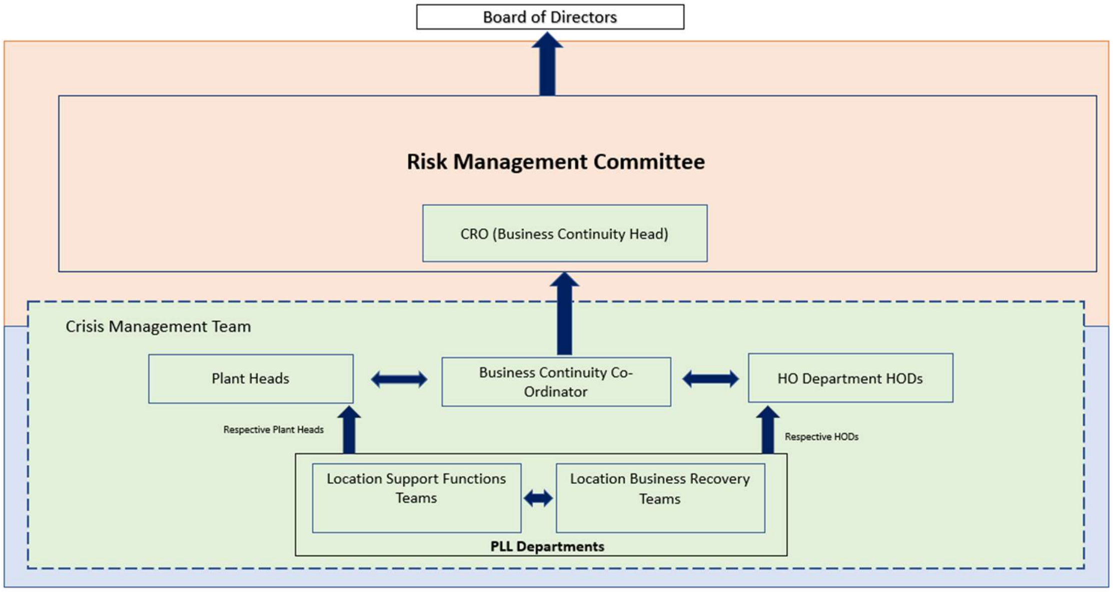

Board of Directors
Risk Management Committee
CRO (Business Continuity Head)
Crisis Management Team
Plant Heads
Business Continuity Co-Ordinator
HO Department HODs
Respective Plant Heads
Respective HODs
Location Support Functions Teams
Location Business Recovery Teams
PLL Departments

Figure 2: PLL BCM Organization Structure

12.1 BCM Roles and Responsibilities

- **Risk Management Committee (Business Continuity management)**

This is the BCM program steering committee, responsible for leading the overall BCMS in PLL and ensuring deliverables are aligned to program objectives. The RMC shall perform yearly review of the BCM program. Their key objectives include, but not limited to:

a) Provide business continuity directives across PLL;
b) Ensuring that the BCMS achieves its intended outcome(s);
c) Review the effectiveness of the program on an annual basis.

To achieve above objectives, following key responsibilities shall be carried out by the RMC.

Responsibilities:

a) Establish the BCMS and set the scope for organization wide BCMS;
b) Setting up objectives & policies for BCMS and ensuring that they are compatible with the strategic direction of the organization;
c) Ensuring management commitment for recovery of processes as per the BCP objective;
d) Ensuring the integration of the business continuity management system requirements into organization's processes;
e) Manage costs associated with business continuity;
f) Provide adequate resources to support and coordinate the implementation of BCMS;
g) Provide direction for the efficient planning and implementation of BCMS recovery strategies and responses;
h) Communicating the importance of effective business continuity management and conformance to the BCMS requirements;
i) Obtain clear understanding of risks and continuity threats to business being faced by the organization and support new initiatives to improve BCMS;
j) Ensure legal and regulatory requirements and contractual continuity obligations are identified, addressed, and achieved;
k) In the event that changes are required to the BCMS policies, provide approval for implementation of changes, as required;
l) Authorize the remediation and improvement actions to be taken for BCM arrangements;
m) Review the executive summary of BCM related audit reports;
n) Actively participate in management reviews and promote continual improvements across functions;

o) Ensuring participation at all necessary levels of management, and administrative and technical staff during the planning, development, testing, modification, and implementation of business continuity policies, plans and procedures.

- **CRO (Chief Risk Officer/BCM Continuity Head)** drives the PLL BCMS program and provides directives for implementing BCMS across the organization. The CRO owns the BCMS and delegates its execution responsibilities to the BCM coordinator.

Responsibilities

a) The CRO (Chief Risk Officer/BCM Continuity Head) is responsible for the formulation, implementation, monitoring and maintenance of BCMS across PLL.
b) Oversee the crisis management operation with BCM Coordinator and provide continuous on-ground support till the crisis is averted;
c) Provides specialist business continuity guidance and advice to business-as-usual projects; and new investments outsourcing and contracts initiatives;
d) Co-ordinates with the corporate BCM arrangements and systems, including incident management, both within PLL and with external agencies;
e) Inform external agencies like regulators, police authorities etc. as and when the need arises. Also liaise with service providers including security agencies, house-keeping agencies & IT service providers;
f) Responsible for developing, maintaining, and overseeing implementation of Business Continuity Management Plans (BCMP). The BCP plans shall be updated based on management inputs and implementation feedback from business recovery teams, plant head and support functions;
g) Regularly update the RMC on the compliance and implementation of business continuity framework;
h) Coordinate periodic business continuity reviews as per the defined frequency;
i) Manage the risk assessment and internal BCP audits and facilitate external audits for adherence to standards such as ISO/IEC 22301:2019 etc.;
j) Track and facilitate closure of business continuity observations/non-conformities identified during the internal/external audits;
k) Review root cause analysis, including the investigations, for the reported business continuity incidents;
l) Measure the effectiveness of the training and awareness program.

- **Business Recovery Team**: Coordinate and support the implementation & maintenance of BCMS in the respective department / function and support the Crisis Management Team at respective locations.

The function heads shall have management authority for the personnel, information assets, equipment, and property, utilized in fulfilling the goals of the program(s) under their direction. The BC functional representatives shall work in cooperation with the BC Co-ordinator for the purpose of recovery of all critical business functions and information resources within the organization.

The BC functional heads shall assign custody of program assets to appropriate staff and ensure that they are provided with appropriate directions to implement the defined procedures. The function-level reviews shall be performed on periodic basis for the progress of the program. Their key objectives include, but not limited to:

a) With the direction & support from RMC, ensure BCM is implemented across PLL;
b) Ensure that the BIA & other BCM activities are performed for all the in-scope processes;
c) Ensure periodic evaluation of BCM program through regular exercising & testing program.

Responsibilities:

a) Establish the BCMS and set the scope for BCMS at function level;
b) Participate in the organization's BIA process to identify business critical processes of the organization;

c) Manage adequate resources to support and coordinate the implementation of BCMS at respective functions;
d) Provide business continuity directives across the function and support for the implementation of BCMS;
e) Conducting regular review and signoff of process-wise RTO, MAO, MBCO in consideration with the requirements of the business users;
f) Identification of risks and continuity threats to business being faced by the function and support new initiatives to improve BCMS;
g) Identify solutions and strategy to meet the RTO, MAO, MBCO under scenarios such as people not available, premises not available, information not available and vendor not available;
h) Identify resources (financial, technology, people, processes) required to operationalize the strategy and solutions;
i) Ensure BIA, Recovery Strategy and BC Plan are documented as per the implementation plan for the critical processes;
j) Ensure the proper planning, development, and establishment of recovery policies and procedures for all files or databases supporting critical functions and are necessary to comply with the guidelines for recovery of critical organization processes;
k) In the event that changes are required to the BCMS provide support for implementation of changes, as required;
l) Ensure and monitor business continuity education, training, and awareness across function;
m) Review internal audit report on BCMS and follow-up on the status of corrective actions taken;
n) Review and monitor major incident reports, together with the results of any investigation carried out;
o) Report the lessons learnt from the incident and update the relevant plans and arrangements;
p) Ensure implementation, review, and monitor the corrective, continual improvement actions determined as a result of the management review;
q) Monitor function-level BCMS performance report;
r) Ensure contractual agreements exist, based on the business impact analysis, for recovery of the organization’s mission critical business functions and information resources, in cases where technical services are outsourced to another agency, or private firm.

- **Support Function Team**: This team consists of SPOCs from support functions. This team would be responsible for assisting the business recovery team, Plant Head (if required) and the BCM Co-ordinator in meeting recovery objectives during a recovery phase.
- **Business Continuity Management Co-ordinator (BCMC)** The RMC shall identify and appoint a Business Continuity Management Co-Ordinator (BCMC). The BCMC shall coordinate and ensure implementation of business continuity framework on an on-going basis. Coordinate with various departments and functions to ensure the implementation of BCMS across PLL. Work closely with the Risk Management Committee (RMC), Chief Risk Officer (CRO), and Business Recovery Teams to align BCMS activities with organizational objectives.
- **Crisis Management Team:** Crisis Management Team acts as a crisis governing body for PLL. This team will assess the overall status of a crisis situation and provide guidance to handle and resolve crisis. This team will determine the overall damage and assist the respective authorities in declaration of the disaster and invocation of the BCP, if required.

11. Business Impact Analysis

PLL shall ensure carrying out of a formal business impact analysis to determine the continuity and recovery priorities, objectives, and targets. This assessment shall be carried out at periodic interval or as and when significant changes happen within the functions and their elements.

The objectives of performing BIA are as below:

1) To identify and prioritize the most time sensitive business functions, and services and ascertain the impact of a disruption on them to facilitate development of BCP based on suitable recovery strategies;

2) To identify the continuity requirements for carrying out the activities under the functions and their elements at acceptable levels;
3) Assess the impact of unavailability of the functions and critical elements under them; and
4) Ascertain the Maximum Acceptable Outage (MAO) for each function functions and critical elements under them.

Following shall be the outcomes of the business impact analysis:

1) Identification of critical elements amongst various critical functions;
2) Maximum Acceptable Outage (MAO), Recovery Time Objective (RTO), and Minimum Business Continuity Objective (MBCO); and
3) Resources required for the recovery of the function and critical elements under them.
4) Business as Usual (BAU) Requirements

Refer PLL BCM BIA Procedure for further information.

12. Business Continuity Strategy

12.1. Determination and Selection

Recovery Strategy is a high level tactical and strategic plan in order to continue business, at a pre-defined level, within a pre-defined time interval, following a business disruption. The identified strategy would often require resources and investments to be made and hence should justify the cost in terms of the perceived benefit. Business Continuity strategy for the identified prioritized activities shall be determined and selected based on the outputs from the business impact analysis and risk assessment.

The Business Continuity Strategy shall be determined to appropriately protect prioritized activities. Strategies to stabilize, continue, resume, and recover prioritized activities including their dependencies and supporting resources, and mitigate, respond to, and manage impacts shall also be determined.

It should be ensured that the strategy includes requisite approvals for the time frames for the resumption of prioritized activities. PLL shall also evaluate the business continuity capabilities of its suppliers, while determining its strategy.

Refer PLL BCM Business Continuity Plan for further information

12.2. Business Continuity Plans

The organization shall establish a documented procedure on how it will continue or recover its prioritized activities within a predetermined timeframe, following a disruptive incident. Each business continuity plan must define:

- Purpose and scope,
- Objectives,
- Activation procedures,
- Implementation procedures,
- Roles, responsibilities, and authorities,
- Communication requirements and procedures,
- Internal and external interdependencies and interactions,
- Resource requirements, and
- Information flow and documentation processes.

A business continuity plan shall collectively contain defined roles and responsibilities for people and teams having authority during and following an incident, it should specify the steps for activating the response and provide details to manage the immediate consequences of a disruptive incident giving due regard to the welfare of individuals, strategic and operational options for responding to the disruption, and prevention of further loss or unavailability of prioritized activities. The plan will provide appropriate internal and external communications protocol, instructions on how and under what circumstances PLL shall communicate with employees and their families, key interested parties, and emergency contacts. The plan will contain information on how PLL will continue or recover its prioritized activities within predetermined timeframes and details of the organization's media response following an incident, by capturing details such as:

- Communications strategy
- Preferred interface with the media
- Guideline or template for drafting a statement for the media, and
- Appropriate spokespeople.

Finally, the plan will detail the process for standing down, once the disaster is over.

Refer Business continuity plans for further information

12.3. Recovery

PLL recognizes the fact that business continuity procedures only address the minimum business continuity objectives, and it needs to return to business as usual at the earliest possible timeframe, following an incident. Towards this end, the organization shall establish a documented recovery plan to restore and return business activities from temporary business continuity measures to normal business requirements, after an incident.

The Recovery plan will provide for a detailed assessment of the situation and its impact, and the determination of tasks, steps or activities needed for recovery.

Refer BC Plans for further information.

13. Exercise and Testing

The organization shall ensure that its business continuity plans and strategies are exercised and tested periodically to ensure that they are consistent with its business continuity objectives and to test the effectiveness of BCP in place.

The Exercise Program of PLL shall be designed to examine its staff's ability to effectively respond, recover and continue to perform assigned critical activities when faced with disruptive scenarios.

It shall consider relevant scenarios based on organization's internal and external issues while deciding the type of exercises and tests as part of the program, a test calendar shall be formulated and published once in two years by the PLL RMC.

The organization shall ensure that its business continuity plans and strategies are exercised and tested periodically to ensure that they are consistent with its business continuity objectives and to test the effectiveness of BCP in place.

Below table capture the various types of tests and frequency of tests:

Test	Frequency
Call Tree test	Annual/ whenever there is a change in the BC plan
Tabletop exercise	Annual/ whenever there is a change in the BC plan
Full/ Partial stress test	Annual/ whenever there is a change in the BC plan
Evacuation drills & emergency response drills	Annual for corporate location; As per regulatory requirements for plant location.

Table 5: Exercise Type and Frequency Matrix

14. Maintenance of BCMS

The organization shall strive to maintain the BCMS by a BCM maintenance program that shall be established at PLL in order to ensure that the organization's business continuity capability remains effective, fit-for purpose and up to date. The maintenance program will help PLL perform planned maintenance of BCMS by taking inputs from tests and exercises, internal audits, and management review as well as unplanned maintenance of BCMS considering lessons learned from incidents and changes within and outside PLL operating environment. PLL RMC under the supervision of CRO (BCM Head) along with BCM coordinator shall manage the maintenance program on an ongoing basis.

15. Performance Evaluation

15.1. Monitoring, Measurement, Analysis and Evaluation

PLL shall evaluate the performance and effectiveness of its BCMS. In order to evaluate the performance and effectiveness of BCMS, PLL shall ensure performance metrics are set, which shall then be monitored, measured, analyzed, and evaluated periodically.

15.2. Evaluation of Business Continuity Procedures

PLL shall ensure that evaluations of its business continuity procedures and capabilities are conducted periodically in order to ensure their continuing suitability, adequacy, and effectiveness.

These evaluations must be undertaken through periodic reviews, audits, assessments, exercising, testing, post-incident reporting and performance evaluations. PLL shall ensure that compliance with applicable legal and regulatory requirements, industry best practices, and conformance with its own business continuity policy and objectives are evaluated at planned intervals and when significant changes occur. When business continuity procedures are activated, following a disruptive incident, a post-incident review must be undertaken, and results recorded. Significant changes arising out of these evaluations should be reflected in the BCP in a timely manner.

15.3. Internal Audit

The organization shall plan, establish implement, and maintain an internal audit program, which shall be based on the results of the risk assessments and the results of previous audits. Internal audits of the organization’s BCMS should be conducted at planned intervals in line with ISO 22301:2019 standard to determine its conformity and provide information to Senior Management on appropriateness and effectiveness of the BCMS as well as to provide a basis for setting objectives for continual improvement of BCMS performance.

16. Management Review

Management review provides PLL RMC with the opportunity to evaluate the continuing suitability, adequacy, and effectiveness of the management system. PLL RMC shall review the organization’s BCMS, at planned intervals, to ensure its continuing suitability, adequacy, and effectiveness.

The management review shall include review of the status of actions and follow-up actions from previous management reviews. Reviewing results of BCMS audits including those of key vendors, status of corrective action and results of exercising and testing will form part of the review. Information on the business continuity performance, including trend analysis of audit results, nonconformities and corrective actions, and performance evaluation monitoring and measurement results will be shared with the RMC during the review.

17. Improvement

17.1. Non-Conformity and Corrective Action

Nonconformity refers to non-fulfillment of a requirement, planning approach, incidents, near misses (near hits) and weaknesses associated with the BCMS. PLL shall implement procedures and controls such as Internal Audit, Incident Response, Performance Evaluation, Exercising and Testing and Competence to identify and take actions to control, correct and deal with the consequences of nonconformities.

When nonconformity is identified, PLL shall evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere. It will be ensured that the corrective actions will be appropriate to the effects of the nonconformities encountered.

PLL shall retain documented information as evidence of the nature of the nonconformities and any subsequent corrective actions taken including the results of such action.

17.2. Continual Improvement

The organization shall use the processes of BCMS such as leadership, planning, and performance evaluation to identify improvement areas and make necessary changes to the BCMS so as to continually improve the suitability, adequacy, or effectiveness of the BCMS.

18. Reference Documents

The guidance to business continuity management implementation is obtained from the following documents:

ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

19. Communication process for external requirements

External organizations may request copies of Business Continuity Management documents for reviews and audit purposes. It is important that this information is handled appropriately when sharing the details outside Petronet LNG Limited as the documents may contain confidential internal information.

In case policy is required for other external requirements such as clients and audits, the same will be made available on the approval from the CRO (BCM Head).

---End of the document---