ऑयल इंडिया लिमिटेड
(भारत सरकार का उद्यम)
Oil India Limited
(A Government of India Enterprise)

Oil India Limited

Risk Management Policy

Document Control

Board Approval	
Meeting No.	**Date**
531	21.04.2022

Table of Contents

1. Introduction

The Risk Management Policy is intended to enable the Company to adopt a defined process for managing its risks on an ongoing basis. An important purpose of this document is to implement a structured and comprehensive risk management process, which establishes a common understanding, language, and methodology for identifying, assessing, monitoring and reporting risks and which provides management and the Board with the assurance that key risks are being identified and managed. This policy is an integral part of ERM framework adopted by the Company. The policies underlined herein define the mechanism by which OIL will identify measure and monitor its significant risks.

RM is a systematic approach to provide reasonable assurance to the Board and the stakeholders on risks associated with the organization; including the risk response strategies adopted by the organization in pursuit of organization's objectives. The RM framework document ("RM Framework") describes the structure, processes, and procedures by which the company will implement RM across all its business activities.

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

The Board is responsible for establishing and overseeing the establishment, implementation, and review of the risk management process. The Board may delegate the responsibility of reviewing the effectiveness of the risk management process.

Review of Policy will be carried out periodically with the changes in business and market circumstances. All changes to the Policy need approval by the Board or by the authority as delegated by the Board.

The policy has been developed in line with the requirements of Companies Act 2013 and SEBI Listing Obligations and Disclosure Requirements (LODR) Regulations 2015, amendment (2018) and (2021), with respect to risk management. (detailed text of regulatory requirement is given in the Annexure I)

2. Background

2.1 Scope

The scope of risk management shall cover significant risks applicable to functions / departments / spheres of Oil India Limited. It shall apply to all levels of Oil India Limited; management, business processes, enabling functions, employees, contractors, business partners, or individuals directly / indirectly associated with Oil India Limited.

All employees of Oil India Limited are required to adhere to this policy.

2.2 Purpose

The purpose of this document is to define the requirements around Risk Management. The document sets out the objectives and accountabilities for risk management within Oil India Limited such that it is structured, consistent and effective.

Key benefits of Risk Management Framework

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

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

Objectives of Risk Management

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

To realize the risk management objectives, the Company aims to ensure that:

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

2.3 Applicability

The framework is applicable across all activities performed by Oil India Limited (OIL) from the date it is approved by the Board and as mentioned on the "Document Control Sheet".

2.4 Administration

Any revision to the framework will be incorporated and applicable only after the approval of the Board.

3. Risk Management Policy

The Company is committed to high standards of business conduct and good risk management to:

- Protect the company's assets;
- Achieve sustainable business growth;
- Take risk adjusted business decisions;

- Safeguard shareholder investment; and
- Ensure compliance with applicable legal and regulatory requirements.

This policy intends to ensure that an effective risk management framework is established and implemented within the Company and to provide regular reports on the performance of that framework, including any exceptions, to the Board of Directors of the Company. This Risk Management Policy complements and does not replace other existing compliance programs.

3.1 Risk Management Objectives

The objective of the RM Policy is to establish a structured and intelligent approach to Risk Management for the company with a view to create a "Risk Intelligent" organization. The broader objectives are:

- Provide a sound basis for good Corporate Governance practices;
- Promote an innovative, risk aware culture in pursuit of opportunities to benefit the organization
- Support the achievement of OIL's mission, vision and strategic priorities in line with its core values
- Identify and pursue existing and new opportunities in accordance with the entity's risk appetite and strategy
- Integrate risk management in the culture and strategic decision-making across the organization
- Establish a risk intelligent framework for the organization
- Establish structured processes for identifying, assessing, responding to, monitoring, and reporting on risk
- Anticipate and respond to changing social, environmental, and legislative condition
- Facilitate compliance with the relevant legal and regulatory requirements and international norms

3.2 Definitions

This Risk Management policy is framed around a common understanding of terminology used in this document:

Risk: Risk is an uncertain event or condition that can have a positive or negative effect on achievement of business goals and objectives.

Enterprise Risk Management: Enterprise Risk Management is a process which involves identifying, assessing, measuring, monitoring, and responding to risks across the enterprise in a way that is aligned with the enterprise's objectives and risk appetite.

Risk Analysis: The process of determining how often specified events may occur (likelihood) and the magnitude of their consequences (impact).

Risk Evaluation: The process used to determine Risk Management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria, to generate a prioritized list of risk for further monitoring and mitigation.

Risk Assessment: Risk assessment is the combined process of Risk Analysis and Risk Evaluation.

Risk Classification: Risk elements are classified into various risk classes, termed as 'risk baskets'. Risks are grouped for better management and control. Each risk class is appropriately defined for the purpose

of common understanding. List of risk classes / baskets along with their definitions is attached as Annexure-I. This list may be modified in future to add/modify new risk classes that may emerge.

Risk Appetite: Risk Appetite is defined as the amount of risk an entity is willing to take, given its capacity to bear risk and its risk philosophy. The Company's Board may provide guidance on its risk appetite in value terms over a period of time, after the process is implemented for a few years.

Risk Category: The broad categories to group risks together form the risk categories. More specifically risks are grouped based on the primary cause of the risk.

Risk Register: Compendium of all risks finalized and detailed with risk definition, KRI, risk mitigation and risk owner.

Risk Impact: Result or effect of an event that may bring a range of possible impacts associated with the event.

Risk Likelihood: The assessment of the probability the risk will occur.

Risk Score: The combined product of risk likelihood and risk impact.

Risk Response: A process of assigning risk owners for each risk; determining the strategy for responding to risks, developing and implementing risk treatment plans.

Mitigation and Contingency plans: Strategies aimed at preventing the occurrence of risk event are called mitigation plans whereas Plan B for risks in case of exigency conditions after the risk play is termed as contingency plans.

Key Risk Indicators: "Key Risk Indicators" are rule based quantitative or qualitative triggers from multiple sources of information for early identification of potentially harmful scenarios.

Risk Dashboards: Periodic reports or MIS for risk reporting.

Risk workshop: A risk workshop facilitate a collaborative approach to brainstorm, identify and assess key risks for the concerned unit with the inclusion of all concerned stakeholders.

Residual Risk: The risk remaining after management has taken action to reduce the impact and/or Likelihood of a risk.

Business Continuity Plan: The Business Continuity Plan is built to anticipate outages and failures (disasters, scandals, pandemics etc.) and to be prepared either to mitigate their effects or hasten the recovery.

3.3 Documentation

Appropriate documentation of each stage of the risk management process should be followed. This framework provides a guide to documentation standards and how they are to be utilized.

The documentation will serve following purposes:

- To demonstrate that the risk management process is conducted properly;
- To provide evidence of a systematic approach to risk identification and analysis;
- To provide a record of risks to support the development of a database of the Company's risks;

- Provide responsible management with risk treatment plans for approval and subsequent implementation for those risks with a residual risk rating in excess of risk tolerance limits;
- Provide accountability for managing the risks identified;
- Facilitate continuous monitoring and review;
- Provide an audit trail; and
- Share and communicate risk management information across the Company.

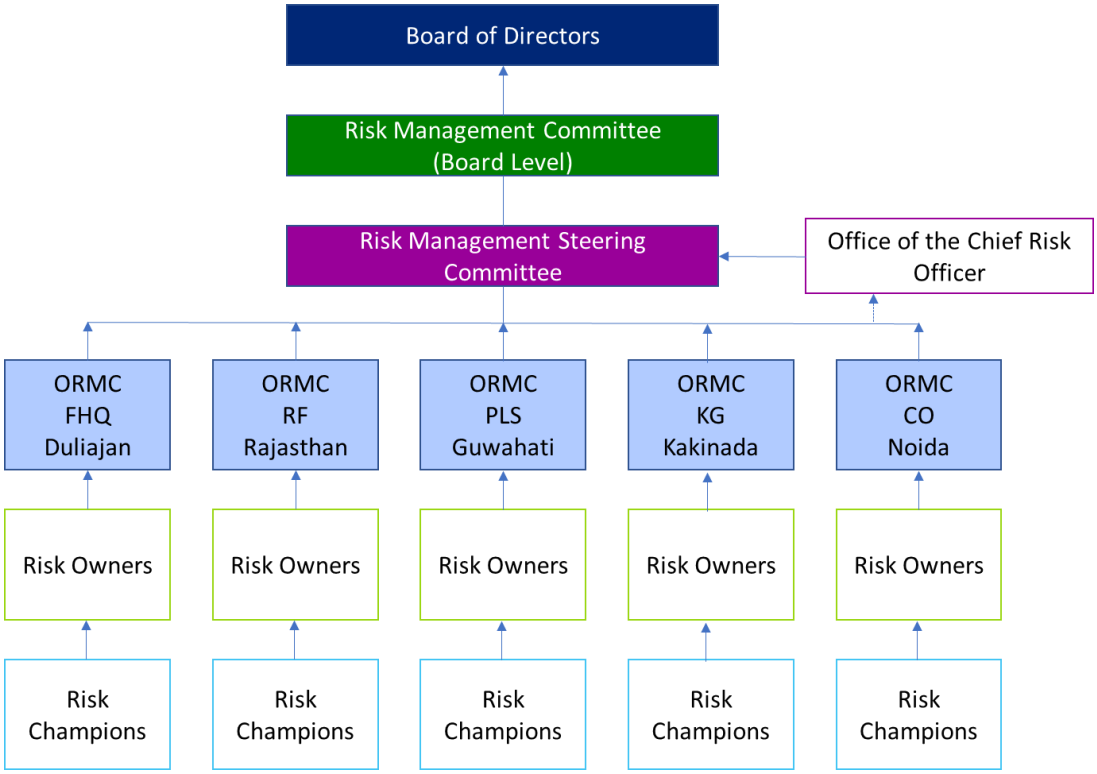
The responsibility for documenting the individual risks has been assigned to the risk owners. Business units are responsible for performing and documenting risk assessments and developing appropriate treatment plans.

The *key documents* pertaining to the risk management process that needs to be maintained by the Company are:

- **Risk Management Policy**: The policy provides the overall framework for Risk Management process of the Company.
- **Risk Register**: It contains list of all risks that have been identified during the periodical review. It is the key document used to communicate the current status of all known risks and is used for management control, reporting and reviews. A Template of the risk register is given as Annexure-III. Risk Registers indicating the risks identified during the Risk Identification workshops for the SBUs / corporate functions have already been issued.
- **Risk Profile**: All risk identified should be profiled. The risk profile provides detailed documentation and attributes of risk along with details of actions planned for risk mitigation. A Template is given as Annexure – III.
- **Risk Management Report**: The Risk Management report is to be placed before the Board for review and approval.

4. Risk Management Organization

The organization structure for risk management is depicted through the flow chart below. Detailed notes on roles and responsibilities of each level follow.



4.1 Board Level Risk Management Committee (Board Level RMC)

Board Level Risk Management Committee shall assist the Board in framing policy, guiding implementation, monitoring, and reviewing the effectiveness of risk management policy and practices. The Committee shall act as a forum to discuss and manage key strategic and business risks. The RMC is chaired by an Independent Director and it shall meet at least twice in a year or at such intervals as may be deemed fit and the roles and responsibilities of the RMC have been defined as per the board approved TOR (Annexure IV)

4.2 Risk Management Steering Committee ('RMSC')

4.2.1 Membership

The Risk Management Steering Committee shall consist of members from the senior executives of the company.

The composition of the Risk Management Steering Committee needs to be approved by the CMD. Constitution of RMSC is subject to change approved by the CMD.

4.2.2 Operation and periodicity of meeting

Functional Director will chair the RMSC. Head of Risk Management – Corporate Office will be responsible as the Convener & Secretary to the RMSC. The RMSC shall meet atleast two times a year (bi-annual basis). Reports of RMSC's activities (agendas, decisions) and meetings (including attendance) will be maintained for each meeting by the Secretary/ Convenor.

4.2.3 Deliverables

At a minimum, the RMSC will deliver:

- Atleast Bi-annual assessment of risks
- Atleast Bi-annual updated Risk Register (including status of mitigation plans) as prepared by the Chief Risk Officer
- Review and recommend to RMC the risk management policy
- Review and recommend to RMC the risk register
- Review and recommend to RMC the Board reportable risks
- Review and approve the mitigation plans
- Review and recommend to RMC new risks, if any and change in priority of existing risks or change in risk statement or dropping existing risk, if any based on changing business environment or as suggested by ORMCs
- Review and recommend to RMC risk mitigation plan of Board Reportable risks
- Oversee recent developments in the company and external business environment and suggest periodic updating of company's risk management program
- Advise ORMCs on changes in risk register based on changing business environment

4.3 Office of the Chief Risk Officer (CRO)

The Office of the CRO (if any) would be responsible as coordinator for Risk Management activity for the entire Company.

The key responsibilities of CRO (if any) will be:

- To ensure that the risk management processes as defined in this policy are executed and to coordinate the effort of various functions/Risk Owners/ Risk Champions/ORMCs to deliver a consolidated view to the RMSC, RMC and Board.
- To facilitate internal risk review meetings, maintaining risk registers, assisting risk owners in identifying and monitoring Key Risk Indicators (KRIs) and risk management policy, and suggesting best practices for strengthening the risk management process
- To ensure that meetings of the RMSC and ORMC are held at minimum bi-annual basis (2 times a year), for the purpose of risk management.
- Ensure periodic review of the risk registers, monitor the risk environment of the company and update risk registers according to regulatory and business requirements defined in this policy.
- To provide periodic updates to the Board, RMC and RMSC on the status of high and new risks and associated mitigation plans.
- To organize awareness sessions regarding Risk Management to ensure the entire organisation is aligned with respect to risk management programs.

4.4 Operational Risk Management Committee ('ORMC')

Chairperson of the respective ORMCs (Field Headquarters Duliajan, Rajasthan Field, KG Basin Kakinada, Guwahati Pipeline, Corporate office Noida) will approve any change in the constitution of concerned ORMC. The Chairperson of ORMC of respective spheres may also invite other members as found necessary to participate in meeting.

4.4.2 Operation and periodicity of meeting

The ORMC shall meet on a bi-annual basis (2 times a year) for urgent matters. Reports of ORMC's activities (agendas, decisions) and minutes of meetings (including attendance) will be maintained for each meeting by the designated convenor of the ORMC.

4.4.3 Deliverables

At a minimum, the ORMC will deliver:

- Atleast Bi-annual (2 times a year) review of risks
- Atleast Bi-annual (2 times a year) updated Risk Register (including mitigation plans)
- Review risk register and status of risk mitigation plans
- Review and approve low & medium risks and mitigation plans
- Review and recommend high risks and mitigation plans to RMSC
- Review, discuss and approve new risks, if any

4.5 Risk Owners and Risk Champions

Risk Owners and Risk Champions need to be assigned for the risks identified during risk identification and assessment process. Risk Owner is attached to a particular risk while Risk Champion is attached to the individual mitigation plan for the risk. Role of Risk Owners, supported by Risk Champions is to assess, review, monitor and react to risks, evaluate and validate the status of risks and propose controls. Risk Owners shall be nominated by the Chairperson, Risk Management Steering Committee, while the Risk Champions shall be nominated by respective Risk Owners.

The Risk Owners and Risk Champions shall meet periodically to discuss new risks added to the risk register during atleast Bi-annual (2 times a year) review and to review the implementation status of mitigation plans. Any risks reassessed as high during the meeting of the Risk Owners/ Risk Champions, shall be escalated to the ORMC/RMSC, as the case may be on an immediate basis.

4.6 Roles and Responsibilities

The Risk Management roles and responsibilities will be as follows:

Board of Directors	• Review the risk appetite, risk management policy, risk register for the company and ensure integrity of risk management systems • Define the roles and responsibilities of the Risk Management Committee and delegate monitoring and review of the risk management framework as deemed fit to the committee • Reporting to Shareholders in Board's report a statement indicating development and implementation of risk management policy for the

	company including identification therein of elements of risk, if any which in the opinion of the Board may threaten the existence of the company • The Board shall oversee risk assessment and minimization procedures and responsible for framing, implementing, and monitoring the risk management plan • The Board of Directors may delegate the responsibility to approve the changes made in risk management policy to meet the regulatory requirements to the Risk Management Committee
Risk Management Committee (Board Level)	• Advise the Board on the effectiveness of the risk management systems atleast annually. • Keep the Board informed about the nature and content of RMC discussions, recommendations, and actions to be taken. Engage other stakeholders in the risk management process when the need is identified. • Formulate a detailed risk management policy which shall include: a) A framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee. b) Measures for risk mitigation including systems and processes for internal control of identified risks. c) Business continuity plan. • Review and approve the Risk Management framework of the Company on a periodic basis. The Committee shall review the risk management culture, processes, and practices of the Company. • Review and recommend for Board's approval the risk profile/ risk register and risk appetite statements • Ensure risk assessment and mitigation procedures are implemented which shall include: a) Formulate measures for risk mitigation b) Oversee the development and implementation of Business Continuity procedures and guidelines c) Monitor and review the exposures of the enterprise level key ("high priority") risk(s), and assess management preparedness to deal with the risk and associated events; d) Ensure that the Company is taking appropriate measures to achieve prudence balance in risk and reward in both ongoing and new business activities; • Monitor and oversee implementation of the risk management policy and ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the

	Company, which shall include: a) Defining the calendar for review of existing risks for each of the functions with the objective to refresh the prioritized risks at defined periodicity; b) Reviewing the key risks for the enterprise at a defined periodicity; c) Refreshing at defined intervals the key risks at the group level so that the Board can refresh the risk review calendar d) Propose enhancements to the RM system, including those required in adherence to changes in regulatory requirements. • Periodically review the risk management policy, at least once in two years, and recommend to Board for approval. • The Committee may form and delegate authority and responsibility to Risk Management Steering Committee (RMSC), which shall assist the RMC to manage the RM activities. • The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the RMC. • Perform any other activities as prescribed under the Listing Regulations and other applicable laws. • The Risk Management Committee shall coordinate its activities with RMSC and Operational Risk Management Committee (ORMC), in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board of Directors
Risk Management Steering Committee	• Review and recommend to RMC the risk management policy • Review and recommend to RMC the risk register • Review and recommend to RMC the Board reportable risks • Review and approve high risks and mitigation plans • Identify new risks if any and change priority of existing risk based on changing business environment • Oversee recent developments in the company and external business environment and periodic updating of company's Risk Management program • Advice ORMCs on changes in risk register based on changing business environment • Receive inputs from risk assessments undertaken namely: Safety and Occupational Risk Management, Financial Risk Management, and Project Risk Management; accordingly, initiate necessary actions to respond to critical risks associated with organization; • Monitor the execution of risk management activities and share best practices among risk practitioners of the organization; • Recommend training programs for staff with specific risk management

	responsibilities to enhance awareness

Office of Chief Risk Officer	• Ensure working of the Risk Management Framework
	• Ensure implementation of risk management policy
	• Responsible to prepare the Risk Management reports for the entire Company
	• Responsible to hold and coordinate the meetings for following committees as per schedule
	  o Risk Management Committee (RMC) at Board Level
	  ▪ Updation on the recommendations of the RMSC
	  o Risk Management Steering Committee (RMSC)
	  ▪ Report to and update the RMSC on risk register and mitigation plans
	  ▪ Report to and update the RMSC on the risk management activities
	  ▪ Monitor emerging issues and share best practices
	  o Operational Risk Management Committee (ORMC)
	  ▪ Ensure that the risk register is reviewed and updated at minimum bi-annually (2 times a year)
	  ▪ Ensure documentation and monitoring of mitigation plans on a periodic basis
	  ▪ Coordinate the risk management initiative for sphere as per the risk management policy and the directives of the Risk Management Steering Committee
	• Assist risk owners in formulation of risk mitigation plans for multi sphere risks
	• Improve risk management process and enhance awareness for the entire company
	• Identify training needs with specific risk management responsibilities

Operational Risk Management Committee	• Review risk register and status of risk mitigation plans • At minimum, bi-annual (2 times a year) updation of Risk Register/ Risk Profile including mitigation plans • Review and approve low and medium risks and mitigation plans • Review and recommend high risks and mitigation plans to RMSC • Review, discuss and approve new risks, if any • Identify Risk Owners for the new risks • Follow directives from RMSC
Risk Owners	• Identify existing control measures • Coordinate the risk management initiative within the department/function as per the risk management framework and the directives of the RMSC/ ORMC;

	• Identify, assess, review and monitor risks within department/function assigned to them; • Provide the necessary support to the Risk Champion in the identification, assessment and reporting of risks in his/her area of operation and resolve differences if any; • Participate in meetings for discussion of risks with risk owners of constituent departments/functions; • Perform ongoing assessment of risks and manage existing risks; • Evaluate and validate the status of risk response plans and propose additional controls/response plans (department and enterprise level risks); • Escalate new risks, as applicable, so that necessary risk assessments can be conducted, as required; • Formulate mitigation plans for Board Reportable Risks for review and recommendation of ORMC • Formulate mitigation plans for other risks, for approval of ORMC • Responsible for managing risk by submitting and implementing mitigation plans shared by Risk Champions • Responsible for addition/deletion of mitigation plan, if any • Ensure that correct and timely risk reports/documentation are maintained and submitted for review
Risk Champions	• Assist risk owner in: o Proposal and formulation of mitigation plans o Documentation of mitigation plans in the risk profile/ risk register document o Implementation of mitigation plans o Report status of implementation

Note: As per terms of reference, Audit Committee will independently review adequacy and effectiveness of risk management activities.

4.7 Periodicity of Activities

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

Roles	Periodicity of Meeting
Operational Risk Management Committee (ORMC)	At minimum two times a year
Risk Management Steering Committee (RMSC)	At minimum two times a year
Risk Management Committee (Board Level)	at least twice in a year (as given in SEBI LODR)
Board of Directors	At least Annually

5. Risk Appetite and Tolerance

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

Establish Risk Appetite and Tolerance Limits:

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

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

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

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

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

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

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

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

6. Risk Management Process

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

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 process and framework adopted by Oil India Limited is mapped as per the ISO Standard 31000:2018 - Risk Management - Guidelines and is in-line with recommendations with the leading practices from COSO Enterprise Risk Management Framework- Integrating with Strategy and Performance and requirements of various applicable regulations in India. Hence, an enterprise wide and comprehensive view will be 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 Oil India Limited has been tailored to the business processes of the organization. Broadly categorizing, the process consists of the following stages/steps:

- Establishing the Scope, Context, Criteria
- Risk Assessment (identification, analysis & evaluation)
- Risk Treatment
- Monitoring and Review
- Communication and consultation
- Recording and Reporting

Figure: Risk Management Process

6.1 Scope, Context and Criteria

Articulate the objectives and define the external and internal parameters to be taken into account when managing risk and sets the scope and risk criteria for the remaining process.

6.1.1 Scope

Risk management process requires setting up a scope which acts as the baseline against the backdrop of which the risks are identified, assessed and treated. Thus, organization should define the scope of its risk management activities. As risk management process is applied at different levels, it is important to clear about the scope, the objectives to be considered and the alignment with organization objectives. Setting up the right scope for the process is of utmost important for a well guided risk management process.

6.1.2 Context

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

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 with and 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
- Consider the risks that will impact the entity's strategy or objectives.

Integration of Strategy with Risk Management: Integration of risk management with business processes is a critical success factor for its functioning. Hence it is ensured that risk management is not isolated from strategy, planning or compliance; rather it is made to be an integral part of the culture itself. The Integration of Strategy with risk management happens in two folds:

Risks TO the execution of the company's strategy - Risks that may impact the execution of the company's stated strategy and/or undermine the Company's ability to achieve or maintain exceptional performance.

Risks OF the company's strategy - Risks that impact the assumptions underlying the company's strategy, challenge the logic of the Company's strategic choices and/or threaten the Company's competitive position.

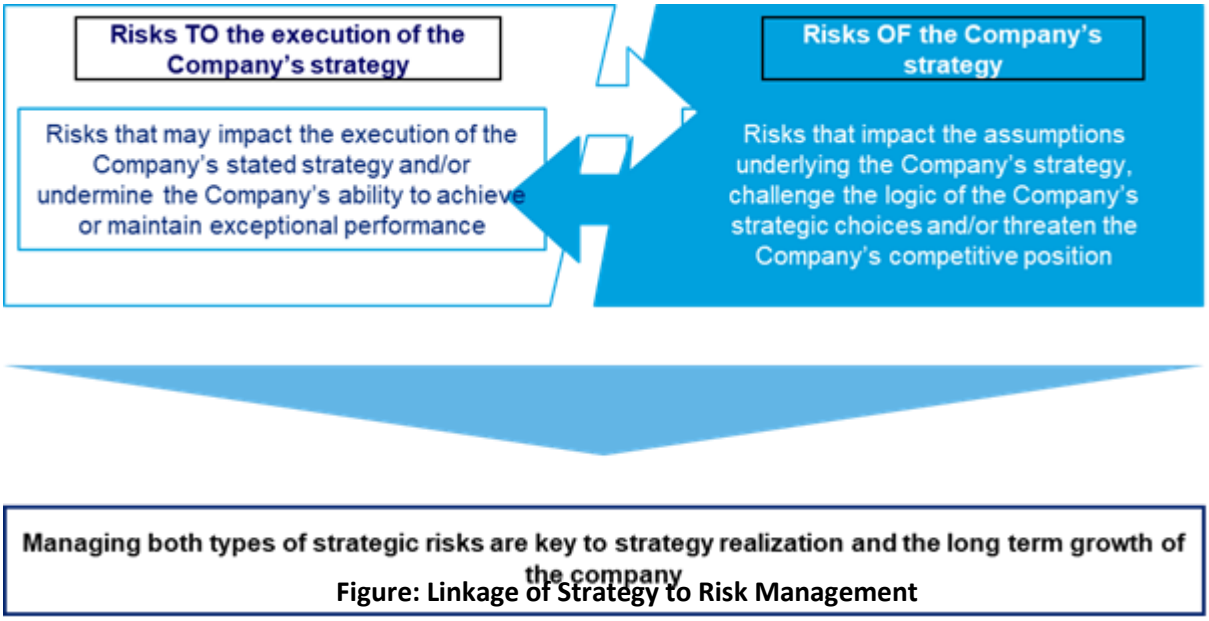


Figure: Linkage of Strategy to Risk Management

The purpose of developing a risk strategy is to articulate clearly how risk should be approached in an organization. Therefore, a strong understanding of the business context, strategy and objectives serves as the anchor to all risk management activities and the effective management of risks.

6.1.3 Criteria

Risk Criteria should reflect the organization values, objectives and resources and be consistent with risk management policies. The criteria should be defined taking into consideration of the organization's obligations and the view of stakeholders.

6.2 Risk Assessment

In order to achieve a comprehensive risk management approach, an organization needs to identify and assess risks that may affect company's ability to achieve its strategy and business objectives.

Risk assessment is the overall process of:

- Risk Identification
- Risk Analysis and Evaluation

6.2.1 Risk Identification

Comprehensive risk identification using a well-structured systematic process is critical, because a potential risk not identified is excluded from further analysis. Identification should include internal and external risks faced by listed entities, including financial, operational, sectoral, sustainability (particularly Environment Sustainability and Governance - ESG -related risks), information, cybersecurity risks and any other risk determined by the RMC. Risks can be identified in a number of ways, viz:

- Structured workshops;
- Brainstorming sessions;

- Occurrence of a loss event;
- Review of documents.

Each Head of ORMC/Function/Location/Risk Owner must periodically review the risks. Workshops or brainstorming sessions may be conducted amongst the focus groups to identify new risks that may have emerged over a period of time. Any loss event may also trigger risk identification.

The broad categories to group risks together form the risk categories. More specifically risks are grouped based on the primary cause of the risk. These may include:

- **Strategic risks:** Risks impacting high-level goals, mission and strategies.
- **Operational risks:** Risks that may disrupt defined business process/operations, lead to inefficient use of resources etc**.**
- **Compliance:** Risks arising out of regulatory non-compliances etc.
- **Financial risks:** Risks impacting financials, increasing cost of operations, leading to stressed books.
- **Cybersecurity:** Risks arising from cyber-attacks or breach within Company's network
- **Sectoral:** Risks originating from the sector and the country in which the Company operates
- **Sustainability (ESG):** Risk relating to ways and means of maintaining a sustainable level of growth without adversely impacting Environment, Health and Safety of the Employees
- **Information:** Risks impacting the integrity of the information used for decision making

All identified risks should be updated in a risk register. Risk registers should be periodically reviewed to ensure pertinence of the risks listed. Risks that would have ceased should also be closed appropriately. The Office of the Chief Risk Officer should ensure that the risk register is reviewed and updated at least 2 times every year.

6.2.2 Risk Analysis and Evaluation

The risks will be assessed Quantitatively on assigned Risk Assessment Parameter (RAP) to measure the current level of the Risk as High, Medium or Low. For each of the Risk, a target number is chosen based on experience, past data, Industry Benchmark and Best Industries Practice.

For example, while assigning the RAP for Risk# Drilling Performance RAP has been arrived at taking into account the Annual MOU Target with MoPNG as well as considering the practical achievable level. If the current level of achievement falls below 92% then it is taken as High, for the range above 92% but below 95%, it is taken as Medium and for range above 95%, it is taken as Low.

Risk Evaluation

The objective of risk assessment and risk evaluation is to assist the organization in prioritizing risk to ensure that appropriate attention is given to risks based on their criticality and that company resources are effectively utilized in managing these risks.

6.3 Risk Treatment / Response Plan

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

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

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

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

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

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

The risk assessed as critical should be profiled in the 'Risk profile/ risk register format' provided in Annexure III. The profile contains details of the risk, its contributing factors, risk scores, controls documentation and specific and practical action plans. Action plans need to be time bound and responsibility driven to facilitate future status monitoring. Mitigating practices and controls shall include determining policies, procedures, practices and processes in place that will ensure that existing level of risks are brought down to an acceptable level. In many cases, significant risk may still exist after mitigation of the risk level through the risk treatment process. These residual risks will need to be considered appropriately. In case of financial risks, this can be accomplished by a combination of:

- Insurance by external agencies; and
- Self-insurance or internal funding.

Escalations of Risks

It is critical to institute an effective system of escalation which ensures that specific issues are promptly communicated and followed up appropriately. Every employee of the Company has responsibility of

identifying and escalating the risks to appropriate levels within the organization. The respective risk owners and office of the Chief Risk Officer will determine whether the risk needs immediate escalation to next level, or it can wait till subsequent periodic review.

Escalation shall enable timely action by appropriate level of management to respond effectively to key risks (critical/severe) faced by the organization.

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

6.3.1 Business Continuity and Contingency Planning

Risks with high velocity/ high impact need to be identified, Business Impact Analysis (BIA) to be performed for such risks and a rapid response plan to be developed for addressing the consequence of the probable risk impact. Contingency plans describe prioritized course of action or actions from different alternatives that may reduce the impact levels of risks for risks with high velocity or high impact and that need to be implemented after the risk event.

Business Continuity Plans are identified in the form of "Contingency Plans" for each risk corresponding to a process/function. Contingency Plans are required to be activated or deployed in case of any emergency or a contingency in the form of a disaster to ensure continuity of the business operations. There are three primary aspects which would be considered as part of Business Continuity Plan:

- **High Availability:** Provide for the capability and processes so that business has access to applications regardless of local failures. These failures might be in the business processes, in the physical facilities or in the IT hardware or software
- **Continuous operations:** Safeguard the ability to keep things running during a disruption as well as during planned outages such as scheduled backups or planned maintenance
- **Disaster recovery:** Establish a way to recover a data centre at a different site if a disaster destroys the primary site or otherwise renders it inoperable.

6.4 Monitoring and Review

Risks and the effectiveness of control measures need to be monitored to ensure changing circumstances do not alter risk priorities. Few risks remain static. Ongoing review is essential to ensure that the management plans remain relevant. Factors, which may affect the likelihood and impact of an outcome, may change, as may the factors, which affect the suitability or cost of the various treatment options.

A risk review involves re-examination of all risks recorded in the risk register/ risk profiles to ensure that the current assessments remain valid. Review also aims at assessing the progress of risk treatment action plans. Risk reviews should form part of agenda for every ORMC meeting. The risk register should be reviewed, assessed and updated atleast on a bi annual (2 times a year) basis.

Office of the Chief Risk Officer is responsible for ensuring that the Risk Register is reviewed and updated at a minimum of biannual (2 times a year) basis.

The frequency of review and reporting of the risk management is given below:

Function	**Frequency**
Risk register/ risk profile	As and when risks are identified and assessed, Bi-annual (2 times a year) basis
Risk assessment	As and when risks are identified, Bi-annual (2 times a year) basis

Annexure I: Regulatory Requirements

❖ SEBI LODR Regulations 2015, Amendment (2018) and (2021)

1. The Board of directors of the listed entity shall have the following responsibilities with respect to risk management:

- Review the Risk Policy [Regulation 4 (2) (f) (ii) (1)]
- Ensure integrity of the Risk Management systems [Regulation 4 (2) (f) (ii) (7)]
- The Board of directors shall ensure that, while rightly encouraging positive thinking, these do not result in over-optimism that either leads to significant risks not being recognized or exposes the listed entity to excessive risk. [Regulation 4 (2) (f) (iii) (9)]
- The Board of directors shall have ability to 'step back' to assist executive management by challenging the assumptions underlying: strategy, strategic initiatives (such as acquisitions), risk appetite, exposures and the key areas of the listed entity's focus. [Regulation 4 (2) (f) (iii) (10)]

2. The listed entity shall lay down procedures to inform members of Board of directors about risk assessment and minimization procedures. [Regulation 17 (9) (a)]

3. The board of directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity. [Regulation 17 (9) (b)]

4. Risk Management Committee [Regulation 21]

- The Risk Management Committee (RMC) shall have a minimum of three members with a majority of them being members of the board of directors, including at least one independent director.
- The Chairperson of the Risk Management Committee shall be a member of the board of directors and senior executives of the listed entity may be members of the Committee.
- The Risk Management Committee shall meet at least twice in a year.
- As provided under Part D of Schedule II, the responsibilities of Risk Management Committee includes formulating of risk management policy, oversee implementation of the same, monitor and evaluate risks basis appropriate methodology, processes and systems and appointment, removal and terms of remuneration of Chief Risk Officer.
- The meetings of the risk management committee shall be conducted in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.
- The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.
- The Risk Management Policy shall include framework for identification of financial, operational, sectoral, sustainability (particularly, ESG related risks), information and cyber security risks, measures for risk mitigation including systems and processes for internal control and Business Continuity Plan.

❖ **The Company's Act, 2013**

- Report by its Board of Directors, which shall include a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company. [Section 134 (3) (n)]
- Independent directors should satisfy themselves that the systems of risk management are robust and defensible. [Schedule IV]
- 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 risk management systems. [Section 177 (4) (vi)]

Annexure II: List of risk clauses/ category

Sr. No.	Risk Category	Definitions
1	Business Continuity	The planning and processes required to maintain the continuity of business activities or recovery response to a disastrous event which may impact the effectiveness of business operations. This includes internal and external activities and processes (e.g. system failures, accidents, fire, flood, government policy etc).
2	Operations	• Risks associated with the production / operational processes, both internal and external, including procurement of raw materials and quality controls. • Risks associated with a lack of defined policies, processes, procedures or delegations of authority at a group, business unit or product area. • This category also includes risks associated with budgeting, management reporting and cost management.
3	Information Technology	The risk that systems are inadequately managed or controlled, data integrity, reliability may not be ensured, inadequate vendor performance and monitoring, system or network architecture not supporting medium or long term business initiatives and strategy, capacity planning not being reviewed on a regular basis resulting in processing failures, risks ofdata or systems migration or interfaces.
4	Human Resource	Risks associated with culture, organisational structure, communication, recruitment, performance management, remuneration, learning & development, retention, Occupational Health & Safety and industrial relations, including supporting systems, processes and procedures.
5	Strategic	Risks associated with strategy development, strategic alliances, business planning, business mix and performance targets.

6	Financial	• Risks related to liquidity / management of cash and risks related to collection of dues from the debtors. • Risks related to Treasury- foreign currency fluctuation, interest rate fluctuation etc. • Risks inadequacy of controls and lack of monitoring leading to fraud etc. • Other risks associated with taxation also form partof this category
7	Legal and Regulatory	Risks relating to non-compliance with legislation, regulations, supervision or internal policies and procedures. • This category also includes risks relating to regulations that may have adverse impact on the company.
8	Brand/ Reputation	This category includes risks associated with brand management and reputation of the company
9	ESG (Environmental, Social and Governance)	This category includes ESG risks include those related to climate change impacts mitigation and adaptation, environmental management practices and duty of care, working and safety condition, respect for human rights, anti-bribery and corruption practices, and compliance to relevant laws and regulations.
10	Sectoral	• Risks originating from the sector and the country in which the Company operates
11	Cyber Security	• Cybersecurity risk is the probability of exposure or loss resulting from a cyber-attack or data breach on the organization
12	Extended Enterprise	Risk of potential disruption caused by events associated to at key third-party organizations.

This list may be modified in future to add/modify new risk baskets that may emerge.

Annexure III: Risk Profile/ Risk Register

Risk Sl. No.				
Risk Sphere/ Location				
Risk Function				
Risk Category				
Risk Statement				
Risk Description/ Risk Contributing Factors				
Risk Tolerance				
Risk Assessment Criteria	**Parameter**	**High**	**Medium**	**Low**
Risk Assessment Status				
Risk Current Rating				
Risk Owner				
Risk Champion				
S.No.	**Existing Control Description**			
1				
2				
3				
4				
S.No.	**Mitigation Plan/ Action Plan**	**Target Date**	**Status of Action Taken on the Mitigation/ Action Plan**	
1				
2				
3				
4				

Note: For completion of risk action plan/ risk mitigation plans, the overall responsibility lies with respective Risk Owner/ Risk Champion.

Annexure IV: Board Level Risk Management Committee Terms of Reference

Preamble

The Board Level Risk Management Committee *(hereafter referred to as the "Committee "or "RMC"),* has been constituted in alignment with the requirements laid down by the Regulation 21 of the SEBI LODR Regulations *(hereafter referred to as "Listing Regulations"),* 2015 and as amended from time to time.

Oil India Limited (*hereafter referred to as the "*Company") has laid down a risk management policy and a framework that informs the Board members about the risk management process. The Board is responsible for reviewing the risk management policy for the Company. The Board of Directors (*hereafter referred to as the "*Board") may delegate the monitoring and reviewing of the risk management plan to the RMC as deemed fit. This section covers the roles and responsibilities of the Risk Management Committee.

1. Primary Objectives

The Committee is constituted by, and accountable to, the Board of Directors of Oil India Limited. RMC shall assist the Board in monitoring and reviewing:

- The risk management plan;
- The implementation of risk management framework of the Company;
- Review key ("high priority") risks applicable to the Company;
- The cybersecurity and data protection risk of the Company and;
- Such other functions as the Board may deem fit, from time to time.

2. Risk Management Committee Composition

The Board of Directors has constituted a sub-committee - Risk Management Committee (Board Level) to assist the Board in framing policy, monitoring and reviewing the effectiveness of risk management policy and framework. The Committee shall act as a forum to discuss and manage key risks. As per Regulation 21 (2) of Listing Regulations;

a) The Committee shall consist of minimum three members;
b) Majority members of the Committee shall be Board members; *and*
c) The Committee shall include at least one independent director.

The Chairperson of the Committee shall be a member of the Board and shall be responsible for overseeing the functioning of the Committee.

3. Quorum

The quorum for a meeting of the Risk Management Committee shall be either two members or one third of the members of the committee, *whichever is higher*, including at least one member of the Board in attendance. *(Regulation 21 (3B) of the Listing Regulations)*

4. Meetings and Reporting

- The Committee shall meet at least twice in a year with a gap of not more than one hundred and eighty days shall elapse between any two consecutive meetings;
- All or any members may participate in a meeting by video conferencing or by other audio-visual means. A member so participating is deemed to be present in person at the meeting and shall be counted for the purpose of quorum at the meeting of the RMC;
- The Secretary to the RMC shall be responsible, in conjunction with the Chairperson for compiling and circulating the agenda and papers for the meeting;
- Formal decisions shall be made by simple majority, in case of equality the Chairperson of the meeting shall have the casting vote;
- The Secretary to the RMC shall prepare minutes of all the meetings of the RMC and shall circulate the same to the Board and RMC for consideration;
- RMC shall report the outcomes of all its meetings to the Board periodically.

5. Roles and Responsibilities of the Committee

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

- Advise the Board on the effectiveness of the risk management systems atleast annually.
- Keep the Board informed about the nature and content of RMC discussions, recommendations, and actions to be taken. Engage other stakeholders in the risk management process when the need is identified.
- Formulate a detailed risk management policy which shall include:
    d) A framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
    e) Measures for risk mitigation including systems and processes for internal control of identified risks.
    f) Business continuity plan.
- Review and approve the Risk Management framework of the Company on a periodic basis. The Committee shall review the risk management culture, processes, and practices of the Company.

- Review and recommend for Board's approval the risk profile and risk appetite statements
- Ensure risk assessment and mitigation procedures are implemented which shall include:
    e) Formulate measures for risk mitigation
    f) Oversee the development and implementation of Business Continuity procedures and guidelines
    g) Monitor and review the exposures of the enterprise level key ("high priority") risk(s), and assess management preparedness to deal with the risk and associated events;
    h) Ensure that the Company is taking appropriate measures to achieve prudence balance in risk and reward in both ongoing and new business activities;
- Monitor and oversee implementation of the risk management policy and ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company, which shall include:
    e) Defining the calendar for review of existing risks for each of the functions with the objective to refresh the prioritized risks at defined periodicity;
    f) Reviewing the key risks for the enterprise at a defined periodicity;
    g) Refreshing at defined intervals the key risks at the group level so that the Board can refresh the risk review calendar
    h) Propose enhancements to the ERM system, including those required in adherence to changes in regulatory requirements.
- Periodically review the risk management policy, at least once in two years, and recommend to Board for approval.
- The Committee may form and delegate authority and responsibility to Risk Management Steering Committee (RMSC), which shall assist the RMC to manage the ERM activities.
- The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the RMC.
- Perform any other activities as prescribed under the Listing Regulations and other applicable laws.
- The Risk Management Committee shall coordinate its activities with RMSC and Operational Risk Management Committee (ORMC), in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board of Directors

6. Powers of the Committee

The Risk Management Committee (Board level) shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

7. Periodic review of the TOR

- The TOR shall be subject to review as may be deemed necessary and in accordance with any regulatory amendments; and
- Any changes to the TOR shall be approved by the Board.

****