NTPC Ltd.

Enterprise Risk Management (ERM) Policy and Procedures

July 2025

Table Of Contents

1. Introduction

1.1. Commitment to Enterprise Risk Management

NTPC recognizes that effective Enterprise Risk Management (ERM) is essential for the long-term success and sustainability of the company. We are committed to integrating risk management throughout the organization, ensuring it aligns with NTPC's strategic goals and operations.

1.2. Overview of the ERM Policy and Procedures

- *Risk, as defined by ISO 31000:2018 (Risk Management - Principles and Guidelines), "is the effect of uncertainty on objectives".*
- *Enterprise Risk Management (ERM) is an integrated approach to proactively manage risks that could affect the achievement of NTPC's vision, mission and objectives.*
- *ERM is aimed at protecting and enhancing stakeholder value by establishing a suitable balance between harnessing opportunities and managing risks.*

1.2.1. NTPC, with its widely diversified business ventures is exposed to multiple risks from strategic, regulatory, operational, financial and other external perspectives. NTPC recognises the importance of adopting a proactive approach to the management of risk to support both the achievement of its goals and compliance with governance requirements and hence it is committed to:

a. Cultivating an organizational mindset that views ERM as a unified responsibility for all employees.

b. Foster an environment within the enterprise that enables proactive identification, management, monitoring and reporting of various risks.

1.2.2. This document "Enterprise Risk Management Policy and Procedure" (hereinafter referred to as the "ERM Manual") serves as the guiding framework for managing risks across NTPC.

1.2.3. NTPC's ERM Manual are drafted in compliance with the following industry standards and regulatory requirements:

a. Risk Management - Principles and Guidelines' developed by the International Organization for Standardization (ISO 31000:2018 - Risk Management Principles and Guidelines)

b. Enterprise Risk Management Framework by the Committee of Sponsoring Organizations (COSO)

c. SEBI (Listing Obligations & Disclosure Requirements) Regulations, 2015

d. Companies Act, 2013

e. Department of Public Enterprises (DPE) Guidelines, as applicable

1.3. Objective

1.3.1. The objective of this ERM Manual is to:

a. Facilitate risk-based decision making by systematically identifying potential events that may affect NTPC and understanding the risks associated with them.

b. Enhance NTPC's ability to withstand and adapt to adverse events by proactively preparing for and effectively managing potential risks, ensuring business continuity and operational stability.

c. Foster an organizational culture that emphasizes risk awareness, encouraging employees at all levels to recognize and address risks proactively.

d. Enable optimized resource allocation by management by focusing on managing critical risks and optimizing expenditures on risk mitigation strategies to balance cost-effectiveness with strategic goals.

1.4. Policy Applicability

1.4.1. This ERM Manual is applicable in its entirety to NTPC as a standalone entity. Furthermore, it shall also be applicable to NTPC's JVs and Subsidiaries to the extent of protecting the interests of NTPC from an investment and reputational perspective.

1.4.2. Any matters of interpretation of this ERM Manual shall be addressed by CP-SPRM.

1.4.3. In case of any conflict between this ERM Manual and any other departmental policies regarding ERM matters, this ERM Manual shall take precedence.

2. ERM Framework Overview

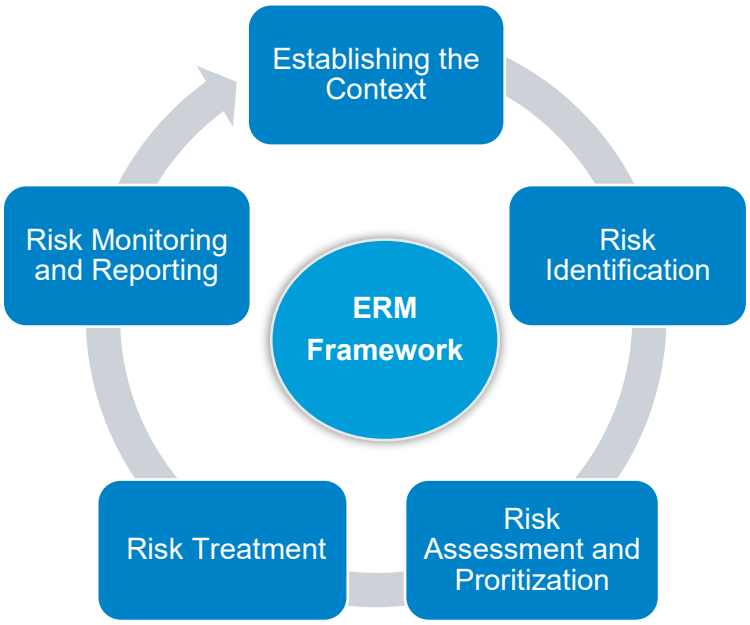


Figure 1: Components of ERM Framework

2.1.1. The following provides a brief description of each component of NTPC's ERM framework**:**

a. **Establishing the context: Establishing t**he context means establishing the horizon in which risks can be visualized. The context of NTPC's ERM is established from the understanding of the external and internal environment in which NTPC operates and

reflects the specific environment of the activity to which the ERM process is to be applied. This step lays down the foundation for risk identification process.

b. **Risk Identification:** Risk identification is the process of finding, recognizing and describing risks that might prevent NTPC from achieving its goals. By using risk Inventory and other techniques, risk identification process finalizes risks which will be described, classified and recorded in the risk register.

c. **Risk Assessment and Prioritization:** Risk assessment and prioritization involves quantification of the NTPC's identified risks to enable prioritization and escalation based on potential impact and likelihood of occurrence of risks that can hinder NTPC's ability to achieve its goals.

d. **Risk Treatment:** Risk treatment involves selecting and implementing measures to align risks with NTPC's Risk Appetite. It involves devising and implementing strategies or specific controls to bring risks within appetite.

e. **Risk Monitoring and Reporting:** Risk monitoring and reporting is a continuous process that facilitates systematically reviewing risks, assessing the effectiveness of mitigation measures and communication of relevant risk information to internal or external stakeholders of NTPC.

3. Risk Appetite

3.1. Overview

3.1.1. Risk Appetite defines the extent of risk an organization is prepared to accept, retain or avoid in order to accomplish its objectives.

3.1.2. Following includes the key advantages of risk appetite:

a. Helps NTPC balance risk and opportunity, ensuring that business decisions align with its goals.

b. Helps prioritize resources for critical risks while avoiding overinvestment in low-impact risks.

3.2. Application of Risk Appetite

3.2.1. The risk appetite serves as benchmark for evaluating and managing risks to ensure alignment with NTPC's strategic goals and stakeholder expectations.

3.2.2. Risk Appetite as a basis for mitigation planning**:**

a. The primary objective of risk mitigation is to manage risks so that they are kept within the defined risk appetite levels. This involves implementing corrective actions, process improvements, and controls to ensure risks align with the appetite.

b. All identified risks are mapped to a risk category which has a defined risk appetite. Mitigation strategies are developed to reduce the impact or likelihood of risks exceeding NTPC's risk appetite levels.

c. Risk owners are responsible for ensuring mitigation efforts align risks with NTPC's defined appetite. Progress on mitigation measures and residual risk levels are regularly reported to the Risk Management Committee (RMC).

4. Risk Reporting Structure

4.1. Risk reporting structure at NTPC

Accountability for enterprise-wide risk management in NTPC resides with the Board of Directors, although responsibility for enterprise-wide risk management is dispersed throughout NTPC under the supervision of the RMC.

NTPC's Risk Reporting structure complies with the following principles:

a. Three Lines of Defence (3LoD) model

b. Three- tiered approach

4.2. Roles and responsibilities

4.2.1. Board of Directors:

a. Approving the ERM Policy, ensuring it aligns with NTPC's goals and regulatory requirements.

b. Defining the organization's risk appetite across key risk groups.

c. Periodically review risk reports and dashboards, as prescribed by SEBI LODR or NTPC's requirement whichever is earlier.

d. Ensuring adherence to SEBI's risk management regulations, including the requirement for listed entities to have a risk management committee (RMC) with defined roles and responsibilities.

4.2.2. Risk Management Committee (RMC)

a. Formulate a detailed ERM Policy which shall include:

   I. A framework for identifying both internal and external risks faced by the listed entity, with a focus on financial, operational, sectoral, sustainability (particularly ESG-related), information, cybersecurity risks, or any other risks determined by the Committee,

   II. Strategies for risk mitigation, including systems and processes for internal controls related to identified risks,

   III. Business continuity plan.

b. Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of NTPC.

c. Monitor and oversee the implementation of the ERM Policy, including evaluating the adequacy of ERM systems.

d. Review the ERM Policy as per the frequency prescribed by SEBI LODR.

e. Keep the Board informed about the nature and content of its discussions, recommendations and actions to be taken.

f. Review and approve the terms & conditions of the appointment of CRO, if applicable.

g. Assign roles and responsibilities to the concerned stakeholders and teams for managing and remediating the enterprise-level risks.

h. Ensure that chosen risk approach is aligned with NTPC's mission, vision and goals.

i. Nominate Steering Committees (i.e. RRSC & CRSC) for identifying, analyzing, evaluating, treating, monitoring, reviewing and communicating all categories of risk including strategic, operational, legal & compliance, financial, technology and environment and social risks.

j. Have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, as required.

4.2.3. Chief Risk Officer (CRO)

a. Design, review, and continuously improve ERM processes.
b. Convene and drive the Corporate Risk Steering Committee (CRSC) meetings.
c. Analyse reported risks and implementation plans, prioritize risks (i.e. Top Risks) and validate residual risk ratings.
d. Prepare enterprise-wide risk reports for presentation to the Risk Management Committee (RMC) and the Board of Directors.
e. Regularly update the Board and RMC on NTPC's ERM status and key risks, providing actionable insights and recommendations.
f. Oversee the implementation and validation of the ERM Policy across all verticals/functions, ensuring significant risks are recognized and managed effectively.
g. Collaborate with Risk Owners and other key stakeholders to maintain the Enterprise Risk Register.
h. Foster a robust ERM culture across NTPC through awareness and capacity-building initiatives.
i. Assist the Board and RMC in developing & refining ERM policies to improve NTPC's resilience and capability.
j. Discuss with CRSC, progress on existing mitigation strategies and formulate mitigation strategies for newly identified risks.

4.2.4. CP-SPRM (Corporate Planning- Strategic Planning & Risk Management)

a. Drive the implementation of the ERM initiative across NTPC under the guidance of the CRO.
b. Consolidate and aggregate risks at the enterprise level for comprehensive risk oversight.
c. Identify and prioritize enterprise-wide risks that could impact NTPC's strategic goals and operations.
d. Develop, communicate, and implement appropriate ERM methodologies, tools, and techniques across NTPC.
e. Establish standardized processes for ERM across all business units and operational lifecycles.
f. Communicate relevant risk-related information with the Internal Audit function pertaining to any emerging risks or any other such information which may be relevant to their scope of work.
g. Promote a culture of risk awareness by educating employees on ERM practices and encouraging proactive engagement.

4.2.5. Corporate Risk Steering Committee (CRSC)

a. Evaluate enterprise-level risks impacting NTPC's operations and strategic goals.
b. Provide inputs for CRO's Risk Report to be presented to RMC.
c. Provide strategic oversight and ensure alignment of ERM practices with NTPC's goals.
d. Monitor and assess the progress of risk mitigation efforts across NTPC.

4.2.6. Regional Risk Steering Committee (RRSC)

a. Evaluate region-specific risks impacting operations and strategic goals.

b. Provide inputs for risk report to CRO and identify enterprise risks if any to be escalated to CRSC.
c. Provide guidance to align ERM activities within the region with NTPC's overall goals.
d. Monitor and assess the progress of risk mitigation efforts within the region.

4.2.7. Risk Owners

a. Promote, support and coordinate ERM within their respective functions.
b. Responsible for identification, assessment, consolidation, reporting and monitoring of the risks related to their respective functions across NTPC.
c. Identify risks at enterprise level, along with the suggested action plans/mitigation measures.
d. Conduct risk assessment and categorize risks based on the risk score.
e. Report identified risks in their functional domain to CRSC and facilitate discussions in the RMC for evolving action plans for effective mitigation measures.
f. Incorporate decisions of RMC in the Risk Register in respect of their identified risks.
g. Implement risk mitigation strategies.
h. Review report of Key Risk Indicators (KRIs), enterprise and functional level risks on a continuous basis.
i. Maintain record of risks, controls, KRI and action plans identified by risk reporters, in their respective risk areas.

4.2.8. Risk Reporters

a. Identify region-specific risks, if any affecting multiple units.
b. Collectively own and manage risks for their respective regions, ensuring alignment with NTPC's ERM Policy.
c. Identify, assess, consolidate, monitor, and report risks specific to their region, providing actionable insights for mitigation.
d. Receive and review the risk reports from Unit Heads, including identified risks, root causes, and related data, and forward relevant insights to Risk Owners.
e. Analyse factors contributing to risk exposure and recommend mitigation measures.
f. Report identified risks in their geographical/functional domain to Risk Owners, along with proposed action plans.
g. Escalate risks, critical trends and exceptions and support requirements to the enterprise level.
h. Engage with process owners and personnel to understand current issues and existing mitigation efforts.
i. Prepare consolidated risk reports for review by Risk Owners and the RMC.

4.2.9. Unit Risk Reporter

a. Maintain the Unit Risk Register and report updates to the respective Risk Reporter or Risk Owner.
b. Identify, conduct preliminary assessments (likelihood and Impact), calculate risk score, risk rating and monitor risks related to individual projects or units, ensuring timely reporting.
c. Update KRIs at unit level.
d. Implement agreed action plans to mitigate the impact of identified risks.
e. Support the Risk Reporter with Risk Assessment.
f. Document risks and related information in the IT-enabled risk reporting tool.

g. Escalate challenges, concerns, or unforeseen developments related to risks in a timely manner.

4.2.10. Unit/Function Risk Coordinator

a. Identify, conduct preliminary assessments and monitor risks related to individual function, ensuring timely reporting.
b. Implement agreed action plans to mitigate the impact of identified risks.
c. Document risks and related information in the IT-enabled risk reporting tool at the project level.
d. Analyse factors contributing to risk exposures and share relevant insights with respective Risk Owner/Unit Risk Reporter.
e. Support the Risk Owner/Unit Risk Reporter in consolidation of reports and risks
f. Assist in implementing action plans approved by the RMC.
g. Periodically update risk indicators and mitigation strategies in coordination with relevant stakeholders.
h. Monitor the progress of identified action plans and ensure timely execution.
i. Oversee the implementation of risk treatment plans to address identified risks effectively.
j. Escalate challenges, concerns, or unforeseen developments related to risks in a timely manner.

4.2.11. Regional Risk Coordinator

a. Assist Risk Reporters in consolidating unit-level risks into the regional risk register.
b. Support planning and execution of RRSC meetings.
c. Act as the key contact for regional risk discussions with the CP-SPRM.
d. Track and report mitigation progress for regional risks.

4.2.12. Risk Working Group

a. Collect and provide accurate risk data from respective units or projects to CP-SPRM if required.
b. Support identification of emerging risks and trends.
c. Ensure alignment of mitigation strategies with unit goals and monitor their implementation.
d. Escalate significant concerns to the Risk Reporters/CP-SPRM/Functional Risk Owners.
e. Promote risk awareness and support capacity-building initiatives.

4.2.13. Internal Audit

a. Provide periodic information, as agreed with CP-SPRM, on key risks, if any identified during their audits.
b. Provides actionable insights and recommendations for improving risk management practices, controls, and processes based on their observations, if any during the audits.

4.3. Three Lines of Defense

4.3.1. NTPC's ERM framework adopts the Three Lines of Defence (3LoD) model across all levels of the organization. The roles and responsibilities under this structure are as follows:

a. **First Line of Defence:**
Units, including plant-level operations and functional teams, are responsible for

identifying, assessing, and managing risks at their origin. This includes maintaining and updating unit-level risk registers, conducting periodic risk assessments, and ensuring adherence to NTPC's risk appetite.

b. **Second Line of Defence:**
The CRO along with CP-SPRM, the Regional Risk Steering Committee (RRSC) and Corporate Risk Steering Committee (CRSC) act as oversight bodies, consolidating and validating risks identified by the First Line. They ensure alignment and adherence with NTPC's ERM framework.

c. **Third Line of Defence:**

- The Internal Audit (IA) function will exchange risk-related information and findings (inputs which may lead to an update in the Risk register or mitigation strategies) directly with the CRO and CP-SPRM as required.
- Risk related information would include any such information identified during IA's audits or actionable insights and recommendations for improving risk management practices, controls, and processes based on their observations, if any.
- The IA function will in turn receive risk-related information from CRO/CP Department which may have an impact on their scope.

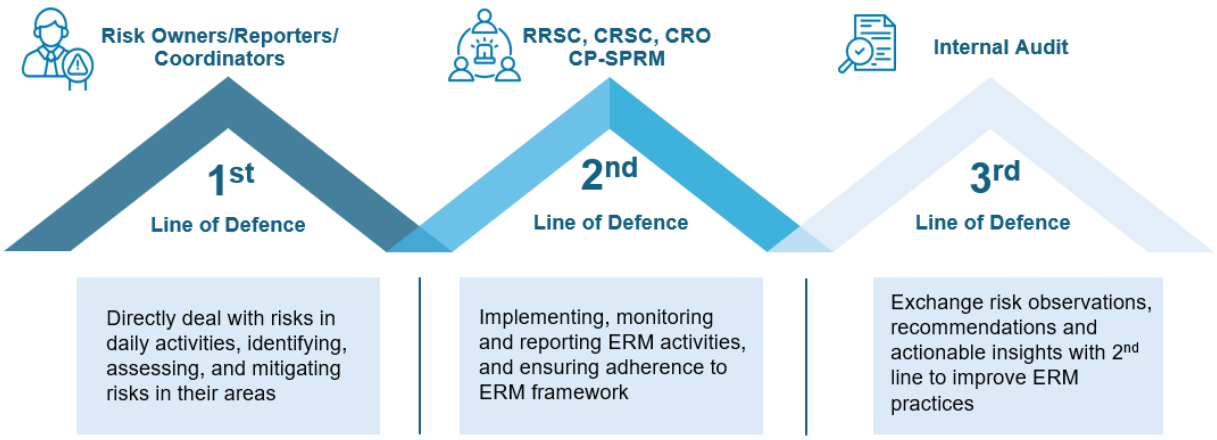


Figure 2 : Three Lines of Defence

4.4. Three-tiered Approach

a. NTPC's ERM framework operates through a three-tiered approach, encompassing Unit, Regional and Enterprise levels. The framework follows a dual methodology, enabling both bottom-up risk identification from units to regions and enterprise levels and top-down risk directives and strategy dissemination from enterprise to regions and subsequently to units.

b. The below figure presents 3 tier levels of ERM framework in NTPC:

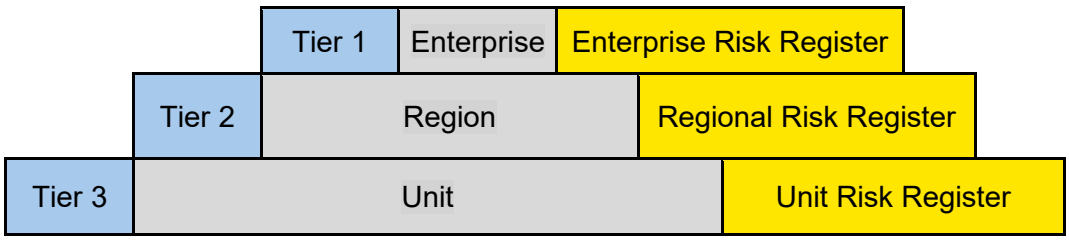


Figure 3 : Risk Identification at all Levels

c. Across the above 3 tiers, NTPC follows both top-down and bottom-up approaches for ERM

5. ERM Procedure/ Process Flow

5.1. Establishing the Context

5.1.1. Overview

The context-setting phase in ERM, (in line with ISO 31000), involves understanding the internal and external environments in which the respective unit operates. It establishes the scope, context, and criteria for managing risks, ensuring alignment with NTPC's goals and informed decision-making. As the foundational step in the ERM process, context setting serves as an iterative process that supports effective risk identification.

5.1.2. Factors to be considered for establishing the context

Factors that influence NTPC's ability to achieve its goals is categorized as follows:

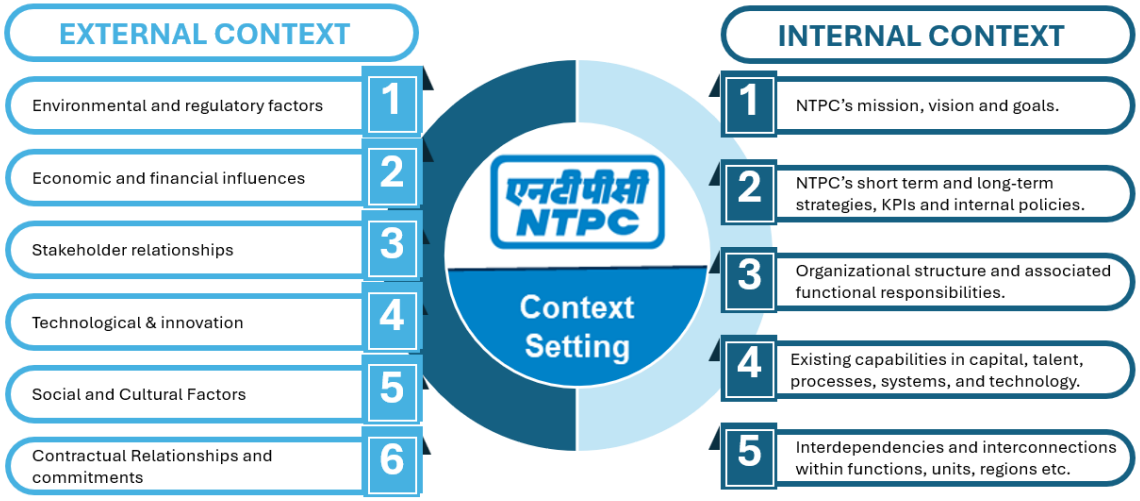


Figure 4: Context setting in NTPC

5.2. Risk Identification

5.2.1. Overview

Risk identification is a structured process aimed at recognizing potential events that may negatively impact the organization's goals, operations, or resources, while systematically describing and classifying the identified risks.

5.2.2. Risk Description

Once risks are identified for, they have to be adequately described in a complete manner containing following three elements:

(i) **Risk event**:
(ii) **Cause of the risk**
(iii) **Impact or consequence of that risk**

5.2.3. Risk Classification

Risk classification enables organizations to systematically identify and group risks, ensuring comprehensive coverage across all functions. Once the risks are described, they are classified into categories of risks to enable structured analysis. The six Risk Groups defined for classifying risks in NTPC's Risk Register are as follows:

a. Strategic Risks
b. Operational Risks
c. Financial Risks
d. Legal & Compliance Risk
e. Environmental and Social Risks
f. Technology Risks

5.2.4. Risk Register

a. Risk Register serves as a comprehensive repository for all identified risks across the organization.
b. Risk register is designed to capture and integrate risk information from various departments and functions, ensuring that risk exposures are not viewed in isolation but rather in the context of their interconnected impact.
c. At NTPC, risk register is maintained at across the following 3 Tiers:
    i. Enterprise Risk Register, maintained by CRO
    ii. Regional Risk Registers, maintained by respective Risk Reporters
    iii. Unit Risk Register, maintained by the respective Unit Risk Coordinator

5.3. Risk assessment and Prioritization

5.3.1. Overview

- Risk assessment and prioritization is a structured approach for systematic evaluation of potential impact of identified risks for NTPC and their subsequent prioritization. This enables informed decision-making and resource allocation.
- NTPC's approach combines both qualitative and quantitative assessment to provide a comprehensive view of risks, guiding the prioritization of management efforts and resource allocation.

5.3.2. Risk analysis

a. Risk analysis evaluates risks by scoring them based on impact (severity) and likelihood (probability) to enable prioritization.
b. Risk analysis involves the following key steps:
    i. Assessment of Likelihood (Probability) of identified risks
    ii. Evaluation of potential impact of identified risks
    iii. Assign risk score for Inherent & Residual risk
    iv. Prioritize risks for further risk treatment

5.3.3. Calculation of likelihood

a. Likelihood assessment

i. Likelihood is the chance of something happening and is determined by the probability of occurrence or potential frequency.
ii. To enable structured and data-driven approach to assessing the likelihood of risk occurrence, likelihood calculation incorporates both historical data and forward looking insights. Thus the likelihood of each identified risk is determined by assigning:
    - Historical score based on how often the risk has occurred in the past
    - Future score based on the likelihood of the risk occurring in the future

5.3.4. Calculation of impact

a. Impact Assessment & Score calculation:

i. **Impact Assessment** involves evaluating the potential consequences of a risk event on varying parameters including strategic, operational, financial and legal.

ii. **Score Calculation** involves quantifying risk impact using predefined criteria (e.g., scale 1-5), often combined with likelihood to derive a total risk score.

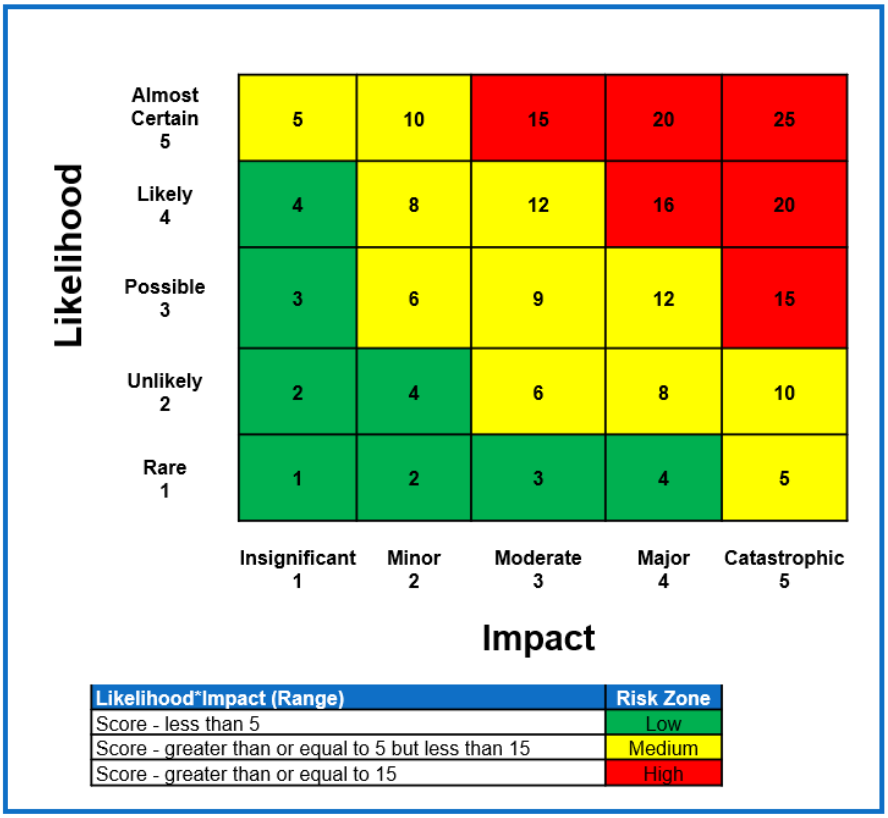
5.3.5. Risk evaluation

a. Output of risk assessment

The risk assessment process generates the following key outputs:

i. **Risk Scoring**

- The scoring provides a quantitative basis for prioritizing risks and determining their criticality.
- Each risk is assigned a score based on its likelihood and impact using the five-by-five matrix provided below:



Likelihood*Impact (Range)	Risk Zone
Score - less than 5	Low
Score - greater than or equal to 5 but less than 15	Medium
Score - greater than or equal to 15	High

Figure 5: 5*5 Risk Assessment Heat Map

5.3.6. Risk prioritization

a. Risk prioritization is the process of systematically ranking identified risks based on their potential likelihood of occurrence and impact.

b. This step is essential for allocating resources effectively and ensuring that top risks are addressed promptly. The prioritization process at NTPC involves:

i. Assessment of Risk Likelihood and Impact

ii. Use of a Risk Matrix

iii. Alignment with Risk Appetite

5.3.7. Risk escalation

a. Risk escalation at NTPC refers to the process of formally raising a risk to higher levels of management when the risk requires further intervention in terms of authority, resources, or expertise.

b. In NTPC's context, escalation may stem from one or more of the following:

   i. Emergence of new risks at Unit / Region / Enterprise level
   ii. Significant change in impact/ likelihood of identified risks causing a change in the risk evaluation
   iii. Unforeseen contingencies

5.4. Risk Treatment

Once the risks are analysed and evaluated, the next step is to treat the risks that are remaining. Risk treatment involves strategies aimed at reducing either the probability or the impact of a risk event by implementing specific controls.

As per NTPC's current ERM framework, following are key risk treatment options which management may adopt to optimise risks:

Risk Acceptance	Risk Avoidance	Risk Mitigation	Risk Transfer
This approach is used when the risks cannot be avoided, reduced, or transferred. NTPC also accepts risks when additional risk mitigation strategies are not cost-effective or when the potential returns	This approach is used for risks where the management may opt to avoid the risks entirely by withdrawing from certain activities (e.g., declining orders, exiting specific regions)	This approach is used to reduce either the probability or the impact of a risk event through the design of specific controls	This approach involves engaging a third party to absorb the impact of the risk event, thereby shifting the responsibility. (e.g. Insurance or joint ventures)

Figure 6 : Key Risk Treatment Options

5.5. Risk Monitoring and Reporting

5.5.1. Overview

Risk Monitoring and Reporting is the process of systematically tracking identified risks, assessing the effectiveness of mitigation measures, and providing timely, structured updates to stakeholders at all levels of NTPC.

5.5.2. Risk reviews

A risk review involves reassessing all risks recorded in the risk register to verify the accuracy of risk scores and its overall relevance. The risk reviews will be conducted on a periodical basis to monitor the effectiveness of NTPC's ERM framework. Table 1 : Risk Monitoring Roles and Reporting Schedule

5.5.3. Key Risk Indicator (KRI) Monitoring and Reporting

KRI Monitoring and Reporting is an integral part of the risk review process, ensuring that risks are continuously assessed based on quantifiable indicators that track early warning signs, emerging trends, and deviations from acceptable thresholds.

5.5.4. ERM Reporting to the Risk Management Committee (RMC)

CRO, supported by the CP-SPRM, will prepare and present a bi-annual ERM report to the Risk Management Committee (RMC). This report will provide a structured and comprehensive overview of ERM activities enabling informed decision-making by the committee.