India Nippon Electricals Limited (INEL)

Risk Management Policy

Table of Contents

1. Background and objectives

1.1 Background

This Risk Management Policy (the 'Policy' or 'RM Policy') intends to enable India Nippon Electricals Limited ('INEL' or the "Company") to adopt a well-defined framework / process for managing pertinent enterprise-wide risks on an ongoing basis, to ensure the Company's objectives are being achieved. The Policy lays out the governance structure and the process to identify, assess, respond, monitor and report on key risks actively and effectively.

The Policy is formulated in compliance with applicable regulations under Companies Act 2013, SEBI (Listing Obligation and Disclosure Requirements) Regulations 2015 and amendments thereof.

The Board of Directors (the 'Board' or the 'BoD') is responsible for development and implementation of an RM Policy, assisted by the Risk Management Committee (the 'RMC'). The Policy should be reviewed at least once in 2 years considering the changing industry dynamics and evolving complexities. Any changes to the Policy should be reviewed and approved by the RMC and the Board.

The Policy complements and does not replace any other existing control, compliance and governance programs.

1.2 Objectives

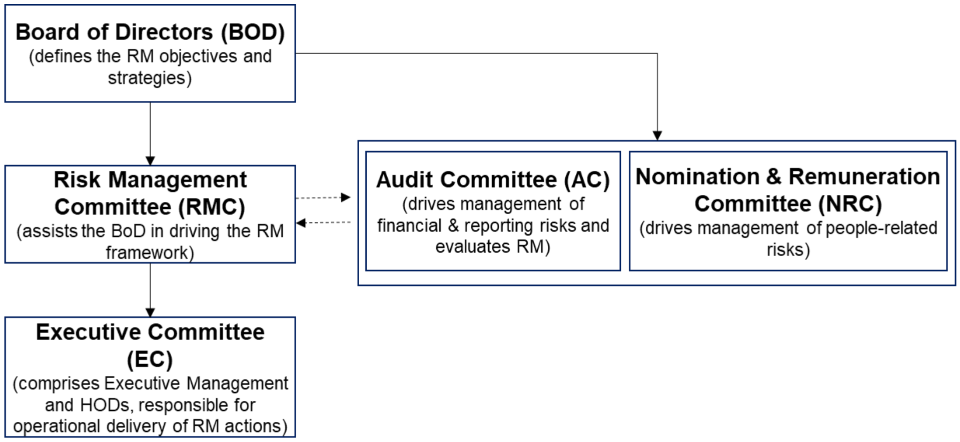
The RM Policy / framework is designed to enable high standards of governance, business conduct and risk management and to achieve the following objectives:

- Informed decision making, adequately factoring risks involved
- Promoting risk-aware culture
- Safeguarding of company's assets and stakeholders' interests
- Achievement of sustainable business growth
- Planning for business continuity
- Compliance with applicable legal and regulatory requirements

2. Risk management governance structure

To ensure high levels of governance and culture, it is important that the risk management framework is driven by exercising adequate Board oversight, establishing operating structures and defining desired culture. The Company's RM framework shall be driven by a 3-tier structure comprising the:

- Board of Directors (BoD)
- Risk Management Committee, along with Audit Committee (AC) and Nomination & Remuneration Committee (NRC)
- Executive Committee (EC)



2.1 Board of Directors (BoD)

The BoD defines the RM strategies & objectives, oversees the development, implementation & operation of the RM Policy / framework and sets the culture for effective risk management.

- The BoD is assisted by the RMC to drive the RM Policy / framework. The BoD has defined the role and responsibilities of the RMC in the form of an RMC Charter and may delegate monitoring and reviewing of the RM framework to the RMC (along with any other functions as it deems fit, including cyber security).
- The BoD has approved the RM Policy and shall approve any subsequent changes thereof, based on bi-annual review and recommendations of the RMC.
- The BoD shall be kept informed by the RMC of the nature and content of the RMC discussions, recommendations and required actions (including status) for key risks. This shall include annual presentations on RM by the RMC, with inputs and support of AC and NRC on management of financial / reporting and people-related risks respectively.
- The BoD shall include a statement in its report to the Shareholders on development and implementation of RM Policy, including identification of elements of any risk, which may threaten the existence of the company.

2.2 Risk Management Committee (RMC)

The RMC was formed by the BoD in Aug-21 to assist in developing the RM Policy, guiding implementation, monitoring, and reviewing the effectiveness of RM Policy and practices. The RMC shall guide and oversee the RM process to identify, assess, manage and monitor key enterprise-wide risks, with inputs from AC & NRC and support from EC.

- **Composition of the RMC:**
  RMC shall comprise minimum of 3 members, with at least 50% being members of the BoD (including at least 1 Independent Director) and remaining members from executive management. Chairperson of RMC shall be an Independent Director.

- **Meetings of the RMC:**

  - RMC shall meet at least twice in a Financial Year, with a gap of not more than 180 days between two such meetings.
  - Quorum required for such RMC meetings shall be the higher of two members (or) 1/3rd of RMC members, including at least one Independent Director in attendance. Participation of the members through video conferencing or other audio-visual means shall be deemed to be adequate for considering quorum.
  - Formal decisions shall be made by a simple majority. In case of equality of votes, the Chairperson of the meeting shall have a casting vote.

  - The Company Secretary shall act as the Secretary to the RMC for the purpose of convening RMC meeting (in conjunction with RMC Chairperson), circulating the agenda & papers and recording & circulating the meeting minutes.
  - RMC may invite any Director, KMP, employee or external experts / professionals to the RMC meetings, as required.
  - Agenda of the RMC meetings may include:
    - review of the Company's RM Policy / framework
    - presentations by EC, relevant risk owners or external consultants on identified / prioritized risks, response plans and monitoring mechanisms
    - compilation of key information / recommendations to be presented to the Board (for direction / action) or the Audit Committee (for evaluation of RM system)
    - presentations by domain / sectoral experts on topics relevant to RM
    - any other topics related to RM.

- **Roles and responsibilities of the RMC:**
  - Formulate a detailed RM Policy which shall include:
    - Framework for identification of internal and external risks specifically faced by the Company, including financial, operational, sectoral, environmental, sustainability, governance, information & cyber security risks and any other risk as may be determined by the RMC.
    - Measures for risk mitigation including systems and processes for internal control of identified risks.
    - Business continuity plan.
    - Any other points that the RMC may find relevant to be included in the Policy
  - Monitor and oversee implementation of the RM Policy, including evaluating adequacy of RM systems and functioning of the ERM framework. This evaluation shall be done at least once in a year considering the risk portfolio.
  - Periodically review the RM Policy (at least once in two years), including by considering the changing industry dynamics and evolving business complexity
  - Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company, including implementing and overseeing an appropriate Enterprise Risk Management (ERM) Framework.
  - Review the identified, prioritized and emerging risks across the enterprise and ensure that they are refreshed at defined intervals.

- Ensure the Company's risk appetite for the purpose of risk assessment and monitoring is appropriately defined.
- Oversee development, implementation and operation of risk responses and provide directions to the EC.
- Review Key Risk Indicators (KRI) dashboards and other performance metrics against prioritized risks.
- Ensure adequacy and effectiveness of Business Continuity Plan and Cyber Security framework.
- Review the adequacy of the Company's resources to perform its RM responsibilities and achieves its objectives.
- Keep the BoD informed about the nature and content of its discussions, recommendations and actions to be taken.
- Appointment, removal and terms of remuneration of a Chief Risk Officer (CRO), if required.
- Coordination of activities with Audit Committee and Nomination & Remuneration Committee, where necessary.
- Engage the services of consultants and other external service providers / subject matter experts and require the attendance of any executives in connection with the RMC's role and shall be entitled to interact with the internal auditors wherever it deems fit and shall also require them to make any presentations thereon.
- Periodically review and recommend the expansion of any power or role of the RMC to effectively perform its role.

2.3 Audit Committee (AC) and Nomination & Remuneration Committee (NRC)

- Audit Committee shall be responsible for periodic evaluation of the RM systems and provide insights / recommendations to the RMC. In addition, the AC would oversee management of the financial and reporting risks faced by the Company, relying on the Internal Financial Controls (IFC) and Internal Audit mechanisms in place.
- Nomination & Remuneration Committee shall oversee management of the people-related risks relevant to the Company and provide insights / recommendations to the RMC.

2.4 Executive Committee (EC)

- Executive Committee (EC) of the Company comprises the Managing Director (MD), President, Chief Financial Officer (CFO), Company Secretary (CS), Chief Technology Officer (CTO) and Heads of Departments (HOD).
- Under the direction of the RMC, EC shall also be responsible for operationalizing the RM Policy and framework including:
  - Developing, implementing and operating an effective Enterprise-wide Risk Management (ERM) framework to identify, assess, manage and monitor risks across risk categories.
  - Directing and overseeing the execution of RM actions by the risk owners / HODs.
  - Keeping the RMC informed of the identified and prioritized risks, risk management actions and results of the risk monitoring mechanisms.
- EC shall meet monthly to review the risk monitoring results / dashboards, emerging risks and status of risk response plans and provide directions to the risk owners / HODs.

2.5 Risk awareness and culture

- Since risk is an integral part of every business activity, the Company aims to embed risk management in its business strategy and operations by promoting risk culture and awareness across the organizations.
- The Company has devised and implemented several risk management programs / measures including Enterprise-wide Risk Management (ERM), Internal Financial Controls (IFC), Internal Audit, Code of Conduct, Whistle-blower Policy and various operational / quality policies.
- Periodic awareness sessions and communications / mailers on risk management, domain and sectoral topics shall be organized for the members of the BoD, the Committees, Executive Management and HODs.
- Periodic awareness communications / mailers on relevant risk management, domain and sectoral topics shall be organized for the wider organization.
- Performance evaluation of the Board, the Committees, Executive Management and HODs shall also appropriately factor performance on risk management activities.

3. Risk management approach

Risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. The Board of Directors are responsible for overall risk management of the company, supported by the Risk Management Committee.

The Company has established an Enterprise-wide Risk Management (ERM) framework to identify key risks across categories / functions, assess the criticality identified risks to prioritize top risks, mitigate / manage the prioritized risks and monitoring the existing & emerging risks.

3.1 Risk identification

- Risk identification shall be carried out across all business verticals / locations of the Company and covering all key risk areas and categories.
- Risk identification shall be performed through internal ideation (such as workshops, brainstorming sessions and inputs from operational reviews), research, inputs from external domain / sectoral experts and any loss event.
- HODs / risk owners shall have the primary responsibility to identify pertinent risks for the Company, with directions / inputs from the EC.
- Risk register (in a pre-defined format) shall be used to compile the identified risks across functions / areas. The risk register shall be reviewed, updated and refreshed periodically.
- Key risk areas / business functions for coverage shall include Business Planning/ Strategy, Marketing & Sales, After-market, Quality, R&D, Engineering, Manufacturing, Maintenance, Finance, Information Technology, Human Resources (including Industrial Relations), Projects, General Administration, Legal & Compliance and Secretarial.
- Key categories of risks for coverage shall include Strategic / Business, Operational, Financial & Reporting, Sectoral, Sustainability (Environmental, Social & Governance / ESG), Technology, Cyber security, Regulatory and Third-party

3.2 Risk assessment

- Criticality of the risks identified across the organization shall be assessed and top / prioritized risks shall be identified based on the risk ratings. This would enable focused approach to risk mitigation / management and monitoring at Management and Committee / Board levels. Such risk assessment should be done periodically to review the relevance of the top / prioritized risks.
- Criticality shall be assessed based on two parameters – Likelihood (probability of risk event occurring) and Impact (consequence of risk occurrence). Based on the Company's risk appetite, risk assessment guidelines shall be developed for both parameters for assessment under the scales below.

Scale	Likelihood
5	Almost Certain
4	Probable
3	Possible
2	Remote
1	Improbable

Scale	Impact
5	Severe
4	Major
3	Moderate
2	Minor
1	Negligible

- The HODs shall have the primarily responsibility to assess the identified risks, with directions / inputs from the EC. Using risk assessment form and referring to risk assessment guidelines, the HODs and Executive Management shall assess each identified risk on the two parameters.
- Criticality score for each risk for each respondent shall be the product of the Likelihood score and the Impact score.
- Risk assessment template (in a pre-defined format) shall be used to compile the criticality responses for each identified risk from various respondents.
- Risk assessment template (in a pre-defined format) shall be used to statistically compute the weighted average criticality scores for each identified risks, assigning 40% weightage to designated risk owners (HODs responsible for the concerned risk area), 40% weightage to designated risk customers (HODs responsible for the functions impacted by the risk) and 20% weightage to other respondents. Based on such weighted average criticality score, the risks are classified into three zones as per the below heat map:
  - Risks with score of 15 & above shall be in the 'red' zone, are considered to have "high" criticality and require active monitoring of risk response and resultant impact. These shall be reviewed by EC monthly and by RMC on half-yearly basis.
  - Risks with score between 8 & 12 shall be in the 'yellow' zone, are considered to have "medium" criticality and need periodic monitoring of risk response. These shall be reviewed by EC half-yearly and by RMC on annual basis.
  - Risks with score below 8 shall be in the 'green' zone, are considered to have "low" criticality and may need bi-annual review of risk response by EC.

Risk Assessment Zone

Likelihood \ Impact	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

High
Needs active monitoring

Medium
Needs annual monitoring

Low
Need bi-annual review

Criticality = Likelihood x Impact

- The risk register (in a pre-defined format) shall be updated with the weighted average criticality scores, rankings and zone.
- RMC shall direct and review the risk assessment approach and outcomes periodically.
- Risk assessment exercise shall be refreshed once in two years to re-visit the prioritized risks

3.3 Risk response

- For the prioritized risks in 'red' zone, root cause analysis shall be performed, existing risk responses shall be evaluated (including process and status) and additional / alternate risk responses shall be identified, by the designated risk owners / HODs considering the Company's risk response strategy and with the directions / inputs from EC.
- The Company may adopt any of the following strategies to respond to a prioritized risk:
  - Risk Acceptance / Retention – Accept and tolerate the risk.
  - Risk Exploitation – Take measures to ensure that the opportunity will be realized.
  - Risk Avoidance / Termination – Take measures which would result in elimination of the risk.
  - Risk Reduction / Mitigation – Take measures which would result in reduction of likelihood or impact of the risk event.
  - Risk Transfer – Transfer some aspects of the risk to a third-party.
- The risk response plan (in a pre-defined format) shall be prepared for each prioritized risk, including the existing measures, additional / alternate measures, responsibility, timelines and status. In addition, the Key Risk Identifiers (KRIs) pertinent to each risk shall be defined, including the source of information and timing / frequency.
- RMC shall direct and review the risk response strategies and plans periodically.

3.4 Risk monitoring and reporting

- Monitoring of status of risk responses: Status of identified mitigation responses for prioritized risks shall be presented by the risk owners to the EC thrice in a year and by the EC to RMC on half-yearly basis. During such reviews, adequacy of the risk responses and need for additional / alternate response plans shall be also assessed.

- Monitoring of Key Risk Indicators (KRI):

    - Key Risk Indicators (KRIs) / performance metrics shall be defined for each prioritized risk, including the relationship with the identified risk, tolerance levels (guided by the Company's risk appetite), source of information, format, timing, frequency and responsibility.
    - Data for each KRI shall be compiled and dashboards / reports of performance shall be prepared as per defined frequency by the risk owners. Based on performance against defined targets / tolerance levels, the status of KRIs shall be marked as 'Green', 'Yellow' or 'Red' for attention / action.
    - Risk owners shall present the KRI dashboards to the EC thrice in a year. Remediation / response plans shall be identified and implemented by the risk owners, with the direction / input from EC.
    - EC and RMC shall present the KRI dashboards (along with remediation / response plans) to the RMC and the Board respectively.

- Identification of emerging risks:

    - Beyond the risks identified through the ERM exercise, it is important to monitor the changing eco-system to identify emerging risks relevant to the Company.
    - Such emerging risks may be identified by the Directors, Executive Management, HODs, employees, customers, vendors, external consultants / experts and any other components in the Company's ecosystem.
    - Under the direction of the RMC, the EC shall develop and implement a mechanism / process to receive and compile inputs on emerging risks from various sources on an ongoing basis.
    - The EC shall monitor and assess potential emerging risks being received and highlight the relevant emerging risks to the concerned risk owners / HODs. After such assessment by HODs and EC, pertinent emerging risks shall be presented to the RMC along with proposed response plans. The relevant risks shall be added to the risk register.

- Review by EC: As explained above in section 2.4, EC shall meet monthly to review the risk monitoring results / dashboards, emerging risks and status of risk response plans and provide directions to the risk owners / HODs.

- Half-yearly review by RMC: As explained above in section 2.2, RMC shall meet at least twice in a financial year, to review the risk monitoring results / dashboards, emerging risks and status of risk response plans and provide directions to EC.

- Annual review by Board: RMC shall report to the Board on annual and need basis on the prioritized risks, related response plans and their KRIs (along with its recommendations for actions), to also aid the Board to include a statement in its report to the Shareholders on development and implementation of risk management.

- Evaluation by AC: Audit Committee shall periodically evaluate the adequacy and effectiveness of the risk management framework in place, through review of risk management reports and actions.

- Integration with Internal Audit:
  - RMC may provide recommendations to the Audit Committee for coverage of certain risk areas / prioritized risks as part of the Internal Audit plan. RMC may also interact with the internal auditors wherever it deems fit and require them to make any presentations thereon.
  - Audit Committee may also mandate the internal auditors to perform a review of adequacy and / or effectiveness of the risk management framework, to aid the AC's evaluation of the RM framework.

4. Business Continuity Planning

- Business Continuity Plans (BCP) and Disaster Recovery (DR) are designed, implemented and operated to enable to the organization to have a rapid response to address the consequence of high impact and high velocity risks. BCP and DR covers key areas such as information technology, assets, manufacturing, supply chain and human resources.
- Documented BCP and DR framework shall be reviewed by the RMC and approved by the Board, including any amendments thereof.
- Reports on operation of BCP and DR framework, including periodic mock drills and testing, shall be presented by the EC to the RMC on annual basis.

5. Annexures

5.1 Risk Register Template

Risk No.	Risk Description	Root Cause No.	Root Cause Description	Contextual Information	Risk Owner	Risk Customer	Weighted Average Criticality score	Criticality Ranking	Criticality Zone	Existing Mitigation Measures	Existing Mitigation Owner

5.2 Risk Assessment Templates

Risk assessment guidelines

Likelihood	Almost Certain (5)	Probable (4)	Possible (3)	Remote (2)	Improbable (1)
History of occurrence					
Probability of future occurrence					

Impact	Severe (5)	Major (4)	Moderate (3)	Minor (2)	Negligible (1)
Parameter 1					
Parameter 2					
Parameter 3					
Parameter 4					

Risk assessment form

Risk Assessment Form

Name			Date of assessment	
Department			Date of Joining	
Designation			Date of starting the Current Role	

Risk No.	Risk Description	Root Cause No.	Root Cause Description	Likelihood Score	Impact Score	Criticallity score

Policy approved by Board on	9th February 2015
Revised Policy approved by Board on	26th May 2022

****