RISK MANAGEMENT POLICY

NAVA LIMITED

(Formerly Nava Bharat Ventures Ltd.)

Regd. Off.: Nava Bharat Chambers, 6-3-1109/1, 3rd Floor, Raj Bhavan Road, Somajiguda, Hyderabad - 500 082, Telangana.

CIN: L27101TG1972PLC001549 T +91 40 40345999, +91 40 23403501 W www.navalimited.com

E nava@navalimited.com; investorservices@navalimited.com

Table of Contents

1. Introduction

1.1. About organization

Nava Limited ("the Company") is a Company domiciled in India, and it was incorporated under the provisions of the Companies Act, 1956. The Company's registered office is situated at Nava Bharat Chambers, 6-3-1109/1 Raj Bhavan Road, Hyderabad – 500 082, India. The Company's equity shares are listed on BSE Limited (BSE) and The National Stock Exchange Limited (NSE). The Company is primarily engaged in the business of manufacture and selling of ferro alloys, Generation of Power, Operation & Maintenance Services for power assets, Mining, Agri and Healthcare Business. The Company operates from its principal place of business located at Paloncha, Hyderabad, Kharagprasad and Samalkot in the states of Telangana, Odisha and Andhra Pradesh, respectively.

1.2. Need for policy

The Company considers risk assessment to be a core component of the Management of the Company and understands that the Company's ability to identify and manage risks to achieve strategic and operational objectives through Enterprise Risk Management Policy.

Enterprise risk management helps organizations to identify events and measure, prioritize and respond to the risks challenging its most critical objectives and related projects, initiatives and day-to-day operating practices. The objective is to protect stakeholders' value through the establishment of an integrated Enterprise Risk Management Framework to provide clear and strong basis for informed decision making at all levels of the organization.

This policy is a formal acknowledgement of the commitment of the organization to risk management. The aim of the policy is not to have risk eliminated completely from the Company's activities, but rather to ensure that every effort is made by the organization to manage risk appropriately to maximize potential opportunities and minimize the adverse effects of risk. The organization aims to use risk management to take better informed decisions and improve the probability of achieving its strategic and operational objectives.

The Policy is formulated in compliance with SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the Listing Regulations") and provisions of the Companies Act, 2013 ("the Act"), which requires:

The Board of Directors of the Company to form a Risk Management Committee (hereinafter referred to as "The Committee / RMC") who shall periodically review this Policy of the Company so that the Management controls the risk through properly defined framework. The Board of Directors may re-constitute the composition of the Committee, as it may deem fit, from time to time.

The Company recognizes that it is exposed to a number of uncertainties, which is inherent for the ferro alloys and power sector that it majorly operates in. The volatility of these sectors affects the financial and non-financial results of the business. To increase confidence in the achievement of organization's objectives, the Company has developed Risk Management Policy to remain a competitive and sustainable organization and enhance its operational effectiveness.

1.3. Objectives of policy

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

The specific objectives of the Risk Management Policy are:

1. To identify business objectives which reflect the interests of all beneficiaries and stakeholders
2. To identify the threats to the achievement of business objectives
3. To regularly review exposure to all forms of risk and reduce it as far as reasonably practicable or achievable
4. To identify and regularly measure key risk indicators and take appropriate action to reduce the risk exposure
5. To regularly review the key risk controls to ensure that they remain relevant, robust and effective
6. To control and manage risk by appropriate risk reduction and mitigation actions

1.4. Risk

Risk[1]: Risk is an event which can prevent, hinder and fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

- Strategic Risk are associated with the primary long-term purpose, objectives and direction of the business.
- Operational Risks are associated with the on-going, day-to-day operations of the enterprise and effective and efficient use of its resources.
- Financial Risks are related specifically to the processes, techniques and instruments utilized to manage the finances of the enterprise, as well as those processes involved in sustaining effective financial relationships with all stakeholders.
- Knowledge Risks are associated with the management and protection of knowledge and information within the enterprise.

2. Risk Governance

2.1. Risk governance structure

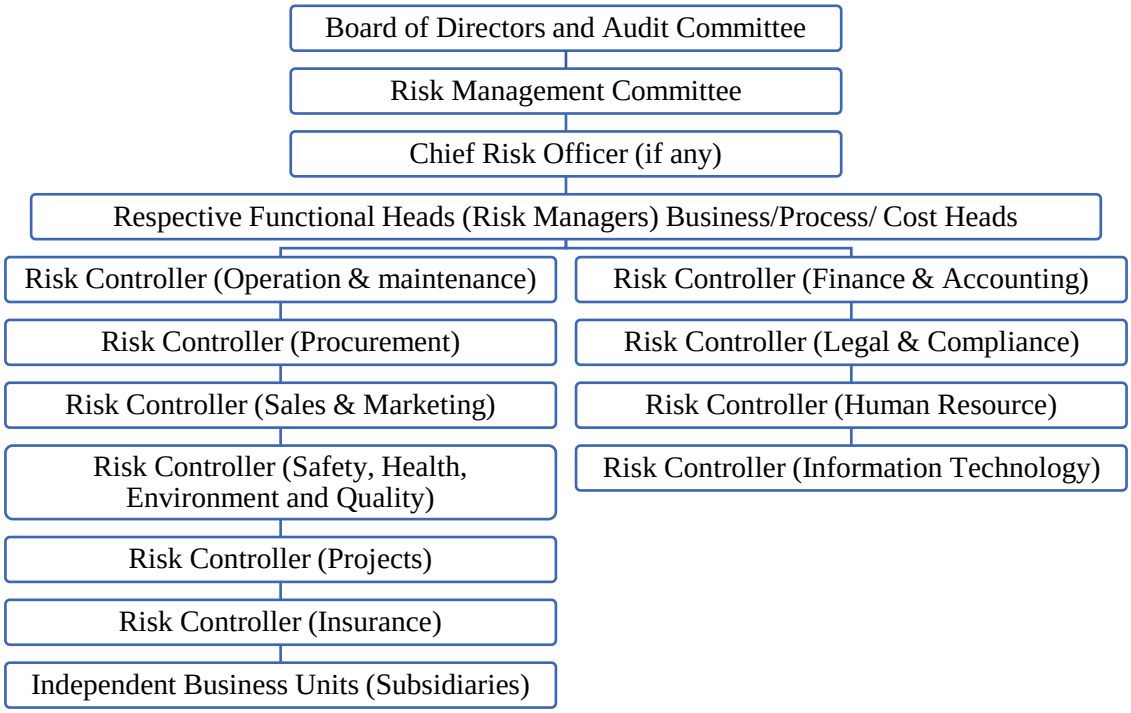
A well-defined risk governance structure serves to communicate the approach of risk management throughout the organization by establishing clear allocation of roles and responsibilities for the management of risks on a day-to-day basis. In order to develop and implement an Enterprise Risk Management framework, the Company shall constitute a Risk Management Committee to be supported by Risk Cell.

[1] as defined in Standard of Internal Audit (SIA) 13 issued by the Institute of Internal Auditors

Risk Management Committee shall identify the key risks and report them to the Board of Directors and Audit Committee, which shall ensure that the risk management activities are undertaken as per this policy. The main objective of the Risk Management Committee shall be to provide an enterprise-wide view of key risks within the organization to the Board of Directors and Audit Committee.

The internal environment reflects an entity's enterprise risk management philosophy, risk appetite, board oversight, commitment to ethical values, competence and development of people and assignment of authority and responsibility. It encompasses the "tone at the top" of the enterprise and influences the organization's governance process and the risk and control consciousness of its people.

The diagram below outlines the risk management structure of Nava Limited and its subsidiaries: -



2.2. Roles and Responsibilities

Board of Directors and Audit Committee:

The Board of Directors ("the Board") and Audit Committee ("AC") shall give directions to the Risk Management Committee on high impact risks and their mitigation. They are also responsible for reviewing and ratifying the risk management structure, processes and guidelines which are developed and implemented by RMC and the Risk managers. The Board and the Audit Committee shall review the periodical risk management reports submitted by RMC.

Risk Management Committee (RMC):

Risk Management Committee is constituted by the Board of directors consisting of such number of Directors (executive or non-executive) as prescribed under the regulations from time to time.

The roles and responsibilities of the RMC as defined by the Board which inter alia, include the following:

1. To formulate a detailed risk management Plan which shall include:
   - A framework for identification of internal and external risks specifically faced by individual departments of the Company and its Subsidiaries.
   - Measures for risk mitigation including systems and processes for internal control of identified risks and business continuity plan.

2. To ensure that appropriate methodology, processes, and systems are in place to monitor and evaluate risks associated with the business of the Company and its Subsidiaries.

3. To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;

4. To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.

5. To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken.

6. The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.

7. 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.

Risk Manager (RM):

The activities relating to risk management is to be managed by a person having overall insight of the Business processes. As such respective business / functional heads are identified as Risk Managers and entrusted with the responsibility of identifying and managing the risks. The Risk Managers are responsible to develop and implement the action plans to address material business and other risks across the Group.

Roles and responsibilities of the Risk Manager are:

- To monitor regularly and evaluate the effectiveness of the action plans and the performance of employees in implementing the action plans.
- To promote and monitor the culture of risk management within the Company and ensure compliance with the internal risk control systems and processes by the employees.
- Regularly report to the RMC regarding the status and effectiveness of the risk management program.
- To carry out any other responsibility entrusted by the RMC from time to time.

Risk Controller:

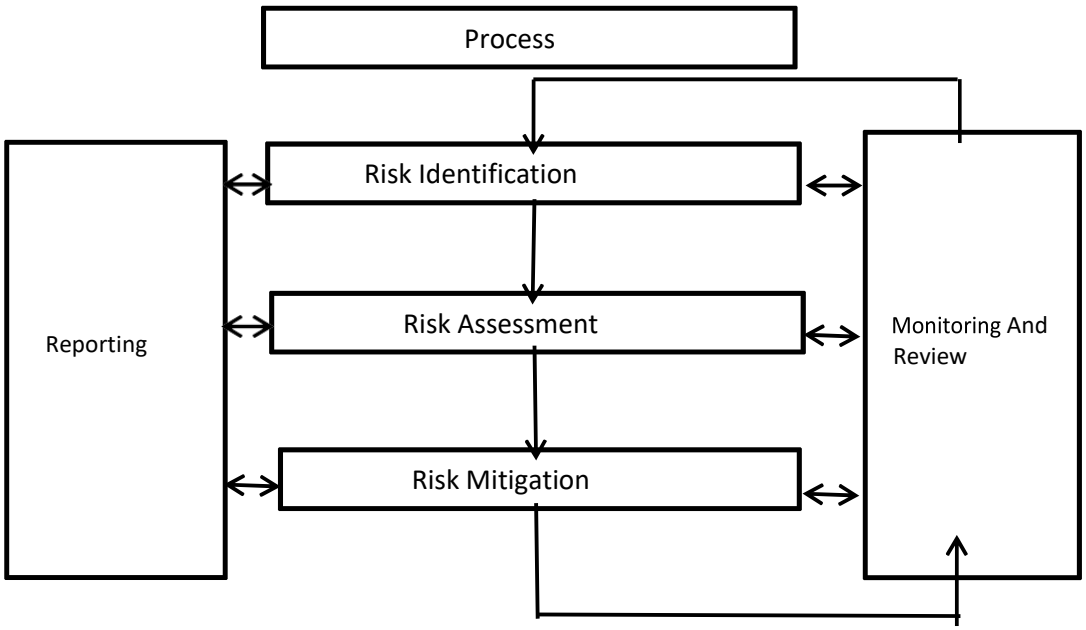
The risk controller of the respective business unit / function will carry out procedures as established by RM and coordinate in reporting key business and other risks across the business unit / function. Key responsibilities of the Risk controller include:

- Identifying and reporting new risks or failures of existing control measures with remedial action.
- Escalation of issues requiring policy approvals and amendments to the Corporate Level.
- Educating employees dealing with key activities of the risk management process.

Employees:
The employees of the Company are directly involved in the business and the functions and as such better placed to identify and manage the risks under the guidance of Risk Controller. They are recognized as important catalyst and are responsible for implementing, managing and monitoring action plans, as appropriate.

3. Risk Management Approach

The Company's risk management framework comprises of a series of processes and guidelines which assist the Company to identify, assess, monitor and manage its business and other risks, including any material changes to its risk profile.
The key elements of the Company's risk management framework are depicted below:



3.1. Risk identification

Risk identification sets out to identify an organization's exposure to uncertain events which may positively or negatively affect an entity's ability to implement its strategy and achieve its objective and performance goals. This requires an in-depth knowledge of the organization, the market in which it operates, the economic, legal, regulatory, social, political, technological and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification shall be approached in a methodical way to ensure that all significant activities within the organization have been identified and all the risks flowing from these activities defined.

The following methodologies can be used to identify risks:

- Brainstorming
- Surveys /Interviews/Working groups
- Experiential or Documented Knowledge
- Risk Lists - Lessons Learned
- Historical risk event information

Company identified the following risks as enumerated below:

External Risk Factors	Internal Risk Factors
• Economic Environment and Market conditions • Fluctuations in Foreign Exchange • Political Environment • Competition or inadequate capacity • Revenue Concentration • Inflation and cost structure • Technology obsolescence • Risk of Corporate Accounting Fraud • Availability or restriction on non-renewable resources.	• Financial reporting risks • Contractual compliance • Compliance with local laws • Quality and Project management • Safety and Environmental management • Human Resource Management • Culture and Values

3.2. Risk categorization

All the risks that have been identified shall be classified under the following risk categories - Strategic, Financial, Operational and Compliance risk.

- **Strategic Risk** - Risk of loss resulting from business factors. These risks adversely affect the achievement of strategic objectives and may impair overall enterprise value.
- **Financial Risk** - Risk directly impacting the balance sheet and access to capital.
- **Operational Risk** - Risk of loss resulting from inadequate or failed processes, people and information systems.
- **Compliance Risk** - Risk of loss resulting from legal and regulatory factors, such as strict privacy legislation, compliance laws, and intellectual property enforcement.
- **Cyber Risk-** Cyber risk commonly refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems.

From the point of view of tracking, risks have further been divided on the business units handling the risk mitigation.

- **Corporate Level Risk** -These risks will be handled by the corporate team and would require mitigation for the entire organization. For e.g., financing, strategy, design risks etc. would need mitigation from corporate offices.
- **Unit Level Risk**- These risks will be handled by respective risk managers and will set the risk management procedures and reporting key risks to the risk management committee as per standard operating procedures

3.3. Risk assessment

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. The events are assessed from two perspectives, likelihood and impact. The positive and negative impacts of potential events are to be examined, individually or by category, across the entity.

Risk Rating is the result of the product of impact and likelihood of occurrence of a risk with the consideration of controls in place.

The risks identified shall be evaluated by their likelihood and impact parameters as per the following methodology:

Impact Rating: Determination of Financial, Operations, Legal & Regulatory impact due to risk occurrence				
Risk Category	**Impact Parameters**	**Measurement Reference**		
		Low (Rating 1)	**Medium (Ratin**	**High (Rating 3)**
Financial	Impact on key company financials such as operating revenue	Insignificant impact on company financial operating revenue (Cost of impact is likely to be less than Rs. 1 Crores p.a.- Less than 0.1%of revenue)*	Moderate impact on company financials operating revenue (Cost of impact is likely to be between Rs. 1-10 Crores p.a.-Between 0.1%-1% of revenue)*	Significant impact on company financials - operating revenue (Cost of impact is likely to exceed Rs.10 Crores p.a.-1% of revenue)*
Strategic	Impact on key strategies for organization such as customers, employees and vendors	Minimum impact on stakeholders	Moderate impact on stakeholders	Significant impact on stakeholders
Operations	Impact on service availability, productivity, third party relationships, brand value and reputation	Minimal impact on operations	Moderate impact on operations	Significant impact on operations
Compliance	Legal and Regulatory breach and its consequences due to non-compliance to legal and regulatory requirements	Minimal or No Impact	Moderate compliance failures detected, limited penalties	Significant compliance failures detected, show cause notice or Significant penalties
Cyber	Impact on reputation of organization or financial loss	Minimal or No Impact	Moderate impact on stakeholders/ financials	Significant impact on stakeholders/ financials

* Materiality levels may change based on scale of operations.

Estimate impact of event:

Process of impact of risk quantification for the company has to be qualitative, supported by quantitative impact analysis. To apply this approach, the chain of adverse consequences, which may occur in case the identified risk materializes, shall be enlisted. For each of the chains of adverse consequences, the cost impact needs to be calculated and attributed to the particular risk. In such an exercise, actual cost impacts as well as opportunity costs must be captured to arrive at the total cost impact of materialization of the risk.

In case, the rating based on different parameters are different, higher of the two or more ratings shall be considered as the final risk rating.

Estimate Likelihood of occurrence:

Process of likelihood of risk quantification for the company has to be qualitative based on Stakeholder discussions and supported by data on the occurrence. To assess the likelihood, the following classification matrix shall be considered as below.

Likelihood Rating: **Determination of Risk occurrence**		
Risk Measurement Score (Likelihood)	**Classification**	**Supplement information to determine the score of Likelihood.**
1	Unlikely	Rare Occurrence based on History
2	Likely	Annual occurrence
3	Very Likely	More than once in a year

Risk Exposure:

The risk assessment methodology adopted defines risk exposure as a product of Impact (rating) of the risk and the Likelihood of occurrence (rating) of the risk.

Impact	x	Likelihood	=	Exposure
(Rating from 1 to 3)		(Rating from 1 to 3)		(Rating from 1 to 9)

The ratings of risk exposure are as follows**: -**

Risk Exposure Rating	
Risk Exposure Score	Classification
<=3	Low
>3 &<=6	Medium
>6 &<=9	High

3.4. Risk mitigation

There are four common strategies for treating risk. There is no single “best” response strategy, and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

- **Risk avoidance/ termination:** This involves doing things differently and thus removing the risk. This is particularly important in terms of project risk, market risk or customer risk but often wishful thinking in terms of the strategic risks.
- **Risk reduction/ treatment:** Reduce or Treat the risk. This is the most widely used approach. The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way through either:
    - Containment actions (lessen the likelihood or consequences and applied before the risk materializes) or;
    - Contingent actions (put into action after the risk has happened, i.e., reducing the impact. Must be pre-planned)

  For managing the Cyber Threats, the Management shall resort to the cost effective IT defensive security measures which may include web filtering, data storage encryption, installing antivirus engines, active patch management, installation of firewall, backup facility(ies), etc. Management in consultation with IT team shall decide the best way to incorporate and implement different types of security procedures in the Company and how to properly train Company staff to obviate cyber security threat.

- **Risk acceptance/ retention:** Accept and tolerate the risk. Risk Management doesn't necessarily mean risk reduction and there could be certain risks within the organization that it might be willing to accept and continue with its operational activities. The Company shall tolerate such risks that are considered to be acceptable,
  for example:

    - a risk that cannot be mitigated cost effectively;
    - a risk that opens up greater benefits than loss
    - uncontrollable risks

  It's the role of Risk Management committees to decide to tolerate a risk, and when such a decision is taken, the rationale behind it shall be fully documented. In addition, the risk shall continue to be monitored and contingency plans shall be in place in the event of the risk occurring.

- **Risk transfer:** Transfer some aspects of the risk to a third party. Examples of risk transfer include insurance and hedging. This option is particularly good for mitigating financial risks or risks to assets.
-

  a) The following aspects shall be considered for the transfer of identified risks to the transferring party:
      - Internal processes of the Company for managing and mitigating the identified risks.
      - Cost benefit of transferring the risk to the third party.

  b) Insurance can be used as one of the instrument for transferring risk.

3.5. Risk Reduction/ Mitigation Process

The risks are identified and the risk mitigation mechanism selected is risk treatment or risk transfer. The nextstep shall be to review and revise existing controls to mitigate the risks falling beyond the risk appetite and also identify new and improved controls.

Risk Mitigation Process:

Control activities are categorized into Preventive or Detective on the basis of their nature and timing:

- Preventive controls - focus on preventing an error or irregularity
- Detective controls - focus on identifying when an error or irregularity has occurred. It also focuseson recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

Evaluate Controls

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite.

Implement Controls

It is the responsibility of the Risk Management Committee to ensure that the risk mitigation plan for each function/department/power station/project site is in place and is reviewed regularly.

3.6. Risk Management and Review

The Risk Management Committee is the key group which shall work on an ongoing basis within the risk management framework outlined in this policy to mitigate the risks to the Organization's business as it may evolve over time.

The Committee identifies, captures and communicates pertinent information from internal and external sources in a form and timeframe that enables the personnel to carry out their responsibilities. Effective communication also flows down, across and up the organization. Reporting is vital to risk management and this component delivers it.

3.6.1 Risk Monitoring

The Risk managers shall be responsible to monitor the mitigation plans as approved and submit the status of the mitigation plan to the Risk Management Committee as and when required.

3.6.2. Risk Review

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place.

Regular audits of policy and standards compliance shall be carried out and standards performance reviewed to identify opportunities forimprovement. It shall be remembered that organization is dynamic and operate in dynamic environment. Changes in the organization and the environment in which it operates must be identified and appropriate modifications made to risk management practices. The monitoring process shall provide assurance that there

are appropriate controls in place for the organization's activities and that the procedures are properly understood and followed.

Any monitoring and review process shall also determine whether:

- The measures adopted resulted in what was intended.
- The procedures adopted and information gathered for undertaking the assessment was appropriate.
- The acceptability of each identified risk and their mitigation plan shall be assessed and risks shall then beranked to identify key risks for the organization.
- Proposed actions to eliminate, reduce or manage each material risk shall be considered and agreed.
- Responsibilities for the mitigation measures for key risks management of each risk shall be assigned toappropriate department/power station/project site heads.

The Risk Managers shall review progress on the actions agreed to mitigate the risk and assess the current level of risk including:

- Establishing whether actions have been completed or are on target for completion.
- Report the status of implementation of mitigation plans to the Risk Management Committee.

Amendment:

Any amendment(s) to this Policy shall be approved by the Board of Directors based on the recommendation of RMC. In the event of any conflict between the Regulations (the Companies Act, SEBI Regulations or any other statutory/ regulatory enactments/ rules/ regulations/ guidelines) and the provisions of this policy, the Regulations shall prevail over this policy.

****