JINDAL STAINLESS LIMITED

CIN: L26922HR1980PLC010901

Corporate Office: Jindal Centre, 12, Bhikaiji Cama Place, New Delhi – 110066

Registered Office: O.P. Jindal Marg, Hisar, Haryana

T: +91 11 41659169, 26101562 E: info@jindalstainless.com Website: www.jindalstainless.com

Enterprise Risk Management Policy

Document properties

Approved by: Risk Management Committee (24.02.2026)

Review frequency: Every 2 years

1. INTRODUCTION

Risk management has always been an integral part of business practices at Jindal Stainless Limited ("the Company"). Effective Enterprise Risk Management (ERM) fosters a culture of risk awareness across all levels to ensure agile, informed decision-making and sustained stakeholder confidence.

The policy provides a structured framework for risk identification, assessment, mitigation, and timely reporting to safeguard stakeholder interests. ERM policy outlines the roles and responsibilities of the Board, Audit Committee, Risk Management Committee & its management.

This policy has been formulated in compliance with Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the Listing Regulations"), and the provisions of the Companies Act, 2013 ("the Act"), which require the Company to establish procedures for risk assessment and risk minimisation. The objectives of ERM policy are to:

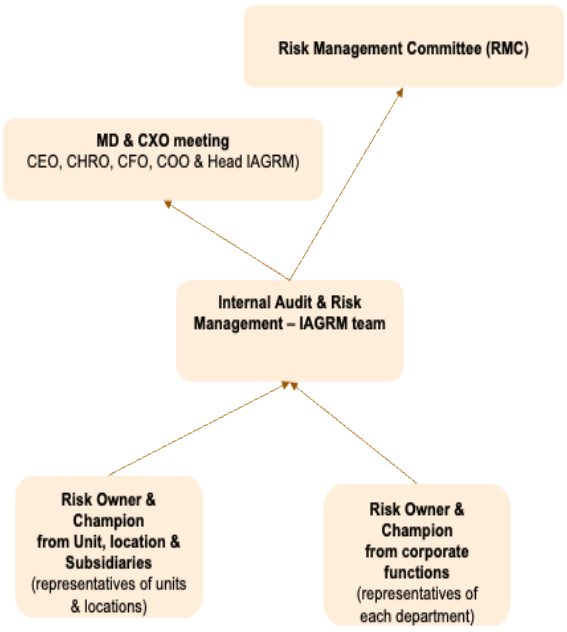
- Establish a common risk management framework across the Company to maintain and enhance the risk management culture.
- Establish ownership throughout the organization and embed risk management as an integral part of the business rather than a standalone system.
- Help the decision makers of the organization explicitly take account of uncertainty, the nature of that uncertainty, and work towards a solution to address it.
- Ensure that all the current and expected risk exposures of the organization are identified, qualitatively and quantitatively evaluated, analyzed and appropriately managed.
- Enable compliance with the relevant legal and regulatory requirements and international norms.

2. RISK GOVERNANCE AND MANAGEMENT

The Board of Directors oversees the Company's risk management framework through the Risk Management Committee (RMC). The RMC holds primary responsibility for overseeing the organisation's exposure to strategic, operational, regulatory, and sustainability-related risks. It conducts periodic reviews of key risks and mitigation strategies and submits its findings and recommendations to the Audit Committee and the Board. Role of Risk Management Committee inter-alia are as follows:

- Monitor and oversee implementation of risk management policy
- Review the results of the risk assessment and mitigation plan development process and Provide guidance on the risk management activities
- Review and monitor the working of the risk management structure and report to the Board of Directors on the status of the risk management initiatives and their effectiveness.
- Review and approve Risk Management Policy at least once in every 2 years

Risk Management structure in the Company is as follows with defined roles across the organisation:



Responsibilities of Each Role in the Organization

MD and CXO will be responsible for fostering an ERM culture throughout the organization, approving risk management models, and reviewing risk mitigation plans.

Risk Owners comprises of the Functions & Unit heads responsible for risk identification, monitoring and risk mitigation.

Risk Champion shall be nominated by the Function & Unit head to assist in maintaining & enhancing ERM capabilities i.e. identification of risk & mitigation plan. The Risk Champion shall also responsible for reporting to Risk Owners and IAGRM regarding risk trends, mitigation plans, issues & any challenges that may arise.

IAGRM will facilitate in identifying & documenting risks and mitigation strategies. It will be responsible for implementing the appropriate ERM framework, reviewing mitigation plans and providing regular updates on risk management to the RMC and CEO/MD.

3. Risk Management framework

ERM framework is built on globally recognised best practices, particularly the COSO (Committee of Sponsoring Organisations of the Treadway Commission) framework, and is tailored to meet JSL's specific business needs. The COSO framework provides a structured and integrated approach to risk management, emphasising the alignment of risk with strategy, performance, and governance. It comprises five interrelated components which collectively support effective risk identification, assessment, and response. This foundation enables the Company to embed risk considerations into strategic planning and operational execution.

The Five Components are as follows:

Governance & Culture

Re-defining control culture and a risk structure using **management oversight** alongside **industry best practices**

Strategy & Objective setting

Analyse business context using **'within & 'outside JSL'** view

Function level analysis & objective setting

Define **Risk appetite**

Performance

Identify **risk at function level & benchmark with industry**

Define Risk response

Risk assessment at impact & likelihood

Review & Revision

Evaluate risk response for mitigating the risk

Update risk on a periodic basis by discussing with function heads

Information, Communication & Reporting

Update to Risk Management committee,

Update the management frequently

4. Risk Assessment Procedure

The Company follows a structured and periodic risk assessment process to identify, evaluate and prioritize risks that may impact the achievement of its strategic, operational, financial, regulatory and reputational objectives.

Key elements of the risk assessment process are as follows:

- **Risk Identification:**
  Risks are identified through a combination of management workshops, business unit assessments, review of internal and external factors, regulatory changes, industry trends, internal audit findings and past incidents.
- **Risk Categorisation:**
  Identified risks are classified under defined categories such as Strategic, Operational, Financial, Compliance etc. as detailed out in section 4.
- **Risk Evaluation:**
  Each risk is assessed based on **Likelihood of occurrence** and **Potential Impact**, considering both inherent and residual risk after existing controls. A standardized risk scoring methodology is applied to ensure consistency. The detailed impact and likelihood methodology is appended below.
- **Risk Prioritisation:**
  Risks are ranked using a risk matrix to identify **Key Risks / Material Risks**, which require enhanced monitoring and management attention detailed out below in a 5x5 matrix.
- **Risk Ownership & Mitigation:**
  Each significant risk is assigned to a designated Risk Owner responsible for implementing and monitoring mitigation actions. Mitigation action is defined on 4T model i.e. Toleate, Treat, Transfer & Terminate
- **Review and Reporting:**
  The risk assessment is reviewed at least annually or upon occurrence of significant internal or external events. Key risks and mitigation status are reported periodically to the Risk Management Committee, Audit Committee and the Board.
- **Continuous Monitoring:**
  The risk assessment process is dynamic and integrated with business planning, internal controls and internal audit to enable early identification of emerging risks

Risk Impact Guideline:

Rating	People	Reputation & Image	Financial	Business continuity	Health & Safety	Customer	Environment	Regulatory/ Legal
Significant 5	Mass layoffs, strikes, loss of critical skills, Attrition > 25%, Absenteeism extensive (>10 days)	Extended global adverse media coverage for more than 7 weeks, and/or significant loss of confidence by stakeholders/ 3rd parties	Revenue impact: >2% of budgeted revenue	Loss of service/ Capacity for more than 5 days	Fatalities, widespread severe health impacts, >10 work-related injuries	Major contract cancellations (>50 Cr), long-term loss of market share	Severe and widespread environmental damage with long-lasting or permanent effects; recovery may not be feasible	Imprisonment, Fines > ₹5 Crores, Revocation of consent to operate
Major 4	High absenteeism (7-10 days), loss of key personnel, Attrition 15-25%	Adverse global adverse media coverage for 5-6 weeks, and/or some loss of confidence by stakeholders/ 3rd parties	Revenue impact: 1-2% of Budgeted Revenue	Loss of service/ Capacity for between 3 to 5 days	Long-term disability, critical injuries, 6-10 work-related injuries	Significant delivery delays or product recalls, loss of key accounts (10Cr to 50Cr)	Significant damage with long-term effects; full recovery may be uncertain even with extensive remediation	Fines ₹1 Crores to ₹5 Crores
Moderate 3	Moderate absenteeism (4-6 days), some staff turnover, Attrition 10-15%	Regional adverse media coverage for 3-4 weeks damaging company brand	Revenue impact : 0.5-1% of Budgeted Revenue	Loss of service/ Capacity for between 2 to 3 days	Medical treatment required, short-term disability, 3-5 work-related injuries	Moderate delivery delays or product quality issues, some loss of customers (1Cr to 10Cr)	Noticeable environmental damage that is reversible over the medium term with active remediation efforts.	Fines ₹10 Lakhs to ₹1 Crores
Minor 2	Minor absenteeism (2-3 days), low impact on morale, Attrition 5-10%	Isolated adverse local media coverage for 1-2 weeks and/or adverse client or stakeholder comments or complaints	Revenue impact : Up to 0.5% of Budgeted Revenue	Loss of service capacity between 1 and 2 days	First aid treatment, no work stoppage, 1-2 work-related injuries	Minor complaints or delays, limited customer dissatisfaction, Customer cancellation (< 1Cr)	Small, localized incidents with minimal harm; quick recovery possible with basic remediation	Fines ₹1 Lakh to ₹10 Lakhs
Insignificant 1	No impact or minor complaints easily resolved, Attrition ≤ 5%, Absenteeism within expected range (0-1 days)	Local press coverage with no or minimal impact, no coverage	Revenue impact : No Impact	Loss of service	No injury or health impact	No impact on customers or easily resolved with standard support	Minimal or no damage; no measurable harm to the environment	Fines up to ₹1 Lakh

Risk Likelihood guideline:

Score	Probability	Description
5	Almost Certain	75% or more chances of occurrence, similar incident has occurred once in past 12 months at JSL.
4	Likely	50% or more chances of occurrence, similar incident has occurred at JSL in past 1-3 yeas
3	Possible	25% or more chances of occurrence, similar incident has occurred in the industry in past 1 year
2	Unlikely	10% or more chances of occurrence, similar incident has occurred in the related sector in past 1 year
1	Remote	Less than 10% chance of occurrence, no known incidents at JSL or within industry peers.

Risk Impact and Risk likelihood when plotted on a Risk Assessment Matrix helps identify the Risk Rating score

Risk Impact	Risk Likelihood				
	Remote 1	Unlikely 2	Possible 3	Likely 4	Almost Certain 5
Significant 5	5 Low	10 Moderate	15 High	20 Severe	25 Severe
Major 4	4 Low	8 Moderate	12 High	16 High	20 Severe
Moderate 3	3 Low	6 Moderate	9 Moderate	12 High	15 High
Minor 2	2 Low	4 Low	6 Moderate	8 Moderate	10 Moderate
Insignificant 1	1 Low	2 Low	3 Low	4 Low	5 Low

5. Risk Category

For better risk identification, the Company categories the risk on the basis of its nature and source. Following categories are defined:

Risk Nature	Definitions
Strategic	Risks that affect the overall goals, direction, and long-term viability of an organization. These include market, competition and reputation
Operational	Risks arising from the internal processes, people, and systems of an organization. These include supply chain, production and labor & cyber security
Financial	Risks related to the financial health of an organization, such as currency, credit and liquidity.
Compliance	Risks associated with the need to comply with laws, regulations, and standards such as legal, environmental and tax.

Risk Source	Definitions
External	Risks beyond the organisation's control: these risks can be unpredictable as they originate outside of the organisation and typically have a low rate of occurrence. Organisations should take actions to cost-effectively reduce the likelihood of occurrence and limit negative effects should the risk event occur. Examples: Geopolitical, Natural Disasters, Competitive Shifts, Tax Laws, etc.

Internal	Internal Risks within the organization's domain: These risks are often associated with the organization's internal environment and can be managed or mitigated through effective policies and procedures. They are generally controllable and can be addressed through internal measures. Organizations should implement strong governance, rigorous controls, and continuous improvement practices to minimize these risks. Examples: Process breakdowns, financial mismanagement, HR challenges, IT system disruptions, etc.

6. Review/Amendment

The Risk Management Committee may recommend to the Board of Directors to amend, modify or revise any or all provisions of this Policy considering the applicable laws from time to time. In case any provision(s) of this Policy is contrary to or inconsistent with the provision(s) of the applicable laws, the provision(s) of the applicable laws shall prevail. Further, amendments in the applicable laws shall be binding even if not incorporated in this Policy.