

THE SANDUR MANGANESE & IRON ORES LIMITED
Enterprise Risk Management Policy

August-2023



Table of Contents

1	Philosophy	3
2	Definitions	3
3	Regulatory Framework.....	4
4	Applicability.....	5
5	Objective and Principles of Risk Management Policy	5
6	Risk Management Governance Structure.....	5
7	Composition of Risk Management Committee (RMC)	6
8	Governance and Risk Management Architecture.....	6
9	Risk Management Framework	10
10	Risk Management Process	10
	10.1 Objective Identification.....	10
	10.2 Risk Identification.....	10
	10.3 Risk Categorization.....	11
	10.4 Risk Analysis and Prioritization.....	11
	10.5 Response to and Mitigation of Risk	13
	10.6 Risk Documentation and Reporting	13
	10.7 Training and awareness.....	13
11	Risk Appetite.....	14
12	ERM Calendar.....	14
13	Risk Management Integration with Other Policies	15
14	Disclosure.....	15
15	Review/ Amendment of the Policy:	15
16	Policy Compliance:	16

Enterprise Risk Management Policy of “The Sandur Manganese & Iron Ores Limited”

‘Risks’ include threats and hazards that can jeopardize success or hinder the performance of tasks. Risk Management comprises of plans and processes to identify risks, evaluate their impacts and steps to avoid, overcome and mitigate or reduce their impacts.

The Sandur Manganese & Iron Ores Limited (“Company”/ “SMIORE”) has prioritized an approach of comprehensive risk management proportionate to the level of risk in the organization, aligned with and embedded into other corporate activities and dynamic to respond to changing circumstances. The Board at its 256th meeting held on 28 October 2005 prescribed a risk management and minimization procedure. Though statutorily, only the top 100 Companies (based on market capitalization) were required to have a Risk Management Committee (RMC), the Board constituted an RMC on 28 May 2014. The RMC was reconstituted on 8 November 2014, 28 May 2016, 6 August 2016, 11 August 2018, 28 May 2019, 5 March 2020 and 10 November 2022. The composition of the RMC has always been in accordance with SEBI regulations.

1 Philosophy

SMIORE is constantly alert to risks and committed to proactively identify, assess and mitigate risks in order to protect its business, improve Corporate Governance and enhance stakeholders’ value.

2 Definitions

1. “**Act**” shall mean the Companies Act, 2013, including the Rules made thereunder, as amended from time to time.
2. “**Applicable Laws**” shall mean the Companies Act, 2013 and the Rules made thereunder, the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 as amended from time to time and such other applicable legislations, rules and regulations.
3. “**Listed Entity or Company or SMIORE**” shall mean The Sandur Manganese & Iron Ores Limited.
4. “**Risk**” is an event, action or inaction that causes a probable threat to the achievement of the objectives of the Company.
5. “**Enterprise Risk Management (“ERM”)**” is the culture, capabilities, and practices, integrated with strategy setting and performance, that a company relies on to manage risk in creating, preserving, and realizing value.
6. “**Impact**” is the potential damage or loss likely to be caused by a risk. The possible impacts may be subdivided into classes according to their severity.

7. **“Likelihood”** is the chance of something happening, measured, or determined quantitatively or qualitatively.
8. **“Risk owner”** is a person with the accountability and authority to manage an identified risk. All the Functional Heads shall be risk owners for their respective areas of operation and the unit heads shall be the risk owners of units.
9. **“Board”** or **“Board of Directors”** shall mean Board of Directors of the Company.
10. **“Policy or this Policy”** shall mean the Risk Management Policy.
11. **“SEBI Regulations”** shall mean the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 together with the circulars issued thereunder, including any statutory modification(s) or re-enactment(s) thereof for the time being in force.
12. **“Stock Exchange”** shall mean a recognized Stock Exchange as defined under clause (f) of Section 2 of the Securities Contracts (Regulation) Act, 1956.

3 **Regulatory Framework**

The key regulations relating to Risk Management are as under:

Regulation	Requirement
The Companies Act, 2013 Section 134 (3)(n)	Directors’ report 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 177 (4)(vii)	Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include: Evaluation of internal financial and operational controls and risk management system.
SEBI (LODR) Regulations, 2015 Regulation 4 (2)(f)(ii)(7)	The Board of Directors shall ensure integrity of the listed entity’s accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.
Regulation 17 (9)(b)	The Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.
Regulation 18 (3)	The Audit Committee shall evaluate the internal financial controls and risk management systems.

Regulation	Requirement
Regulation 21	Constitution of Risk Management Committee of Board of Directors, its roles and responsibilities and frequency of meeting.

4 Applicability

This Policy shall apply to all strategic and operational areas of the Company and its subsidiary. This policy shall be effective from the date of the Board's approval i.e., 3 August 2023.

5 Objective and Principles of Risk Management Policy

SMIORE recognizes that risk is inherent to any business activity and that managing risk effectively is critical to the immediate and future success of the Company. This policy aims to raise awareness of and proactively promote reporting, evaluating, resolving and mitigating risks so as to ensure sustainable business growth with stability. This policy establishes a structured and disciplined approach to risk management, in order to guide decisions and actions on risk related issues, based on the following operating principles:

- a) Make risk management a dynamic, iterative and responsive function focused on value creation for the Company;
- b) Enhance value creation by dealing with uncertainties;
- c) Establish communication and collaboration between the Board and the Management;
- d) Embed risk mitigation in the Company's culture, without discouraging risk taking in furthering the business of the Company; and
- e) Put in place risk management strategies, processes and approaches that:
 - Cover every scope of the entire business including but not limited to strategic and operational areas
 - Address the full spectrum of risks
 - Focus on the probability of and vulnerability to different risks, address adverse consequences and multiplier effects of a combination of several risks
 - Make strategic decisions based on risk informed processes

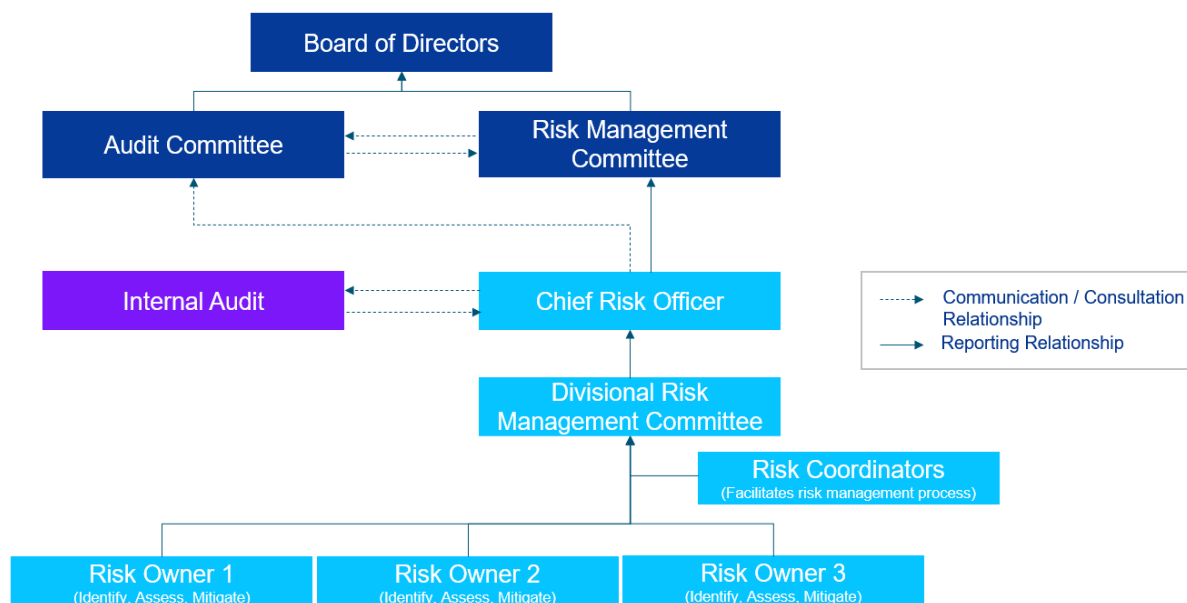
6 Risk Management Governance Structure

The Risk Management Governance structure identifies key internal stakeholders responsible for creating, implementing and sustaining the ERM initiative in the Company. The governance structure leverages the existing organizational structure in the Company.

The governance structure aligns individuals, teams and departments with the intent of establishing responsibility and accountability with regard to:

- Integrating ERM into the Company's culture and strategy management
- Facilitating and monitoring effective implementation of the ERM framework
- Ensuring that the ERM framework and its components are current

The overall structure and roles for the ERM function is summarized below:



7 **Composition of Risk Management Committee (RMC)**

In accordance with Regulation 21 of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, SMIORG continues its existing Risk Management Committee as constituted periodically, which fully complies with the said regulations. In case of any amendment or modification of the SEBI regulations, the RMC shall be re-constituted accordingly.

The RMC shall meet at least twice in a year in such a manner that not more than one hundred and eighty days shall elapse between any two consecutive meetings. The quorum for a meeting of the RMC 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 of Directors in attendance.

The details of the RMC composition shall be hosted on the Company's website at www.sandurgroup.com.

8 **Governance and Risk Management Architecture**

The following are the key roles and responsibilities of various levels regarding risk identification, assessment, mitigation and monitoring:

Level	Key Roles & Responsibilities
Board of Directors	<ul style="list-style-type: none"> Approve and review the Risk Management Policy at least once in every two years Assess the appropriateness of entity's strategy, alignment to

Level	Key Roles & Responsibilities
	<p>mission, vision, and core values and the risk inherent in that strategy</p> <ul style="list-style-type: none"> • Review the entity’s strategy and underlying assumptions against the portfolio view of risk • Define the roles and responsibilities of the RMC and delegate monitoring and reviewing of the risk management plan to the Committee and such other functions as it may deem fit • Establish a risk mitigation culture and determine the risk appetite of the Company • Frame, implement and monitor the risk management plan and policies on the recommendation of RMC • Ensure that appropriate systems for risk management are in place • Continually monitor the management of strategic risks
Audit Committee	<ul style="list-style-type: none"> • Review the status and effectiveness of Risk management policy implementation • Review on a periodic basis the status of enterprise risks • Evaluate internal financial controls and risk management systems • Review financial and reporting risks • Review commodity price risk, foreign exchange risk and hedging activities • Review incidents related to fraud, security, financial losses and any other events impacting the business or reputation
Risk Management Committee	<ul style="list-style-type: none"> • Oversee and monitor implementation of the risk management policy, including evaluating the adequacy of risk management systems • Review strategic risks arising out of adverse business decisions and lack of responsiveness to changes • Review emerging risks and significant changes to the portfolio view of risk • Review operational risks including cyber risks and business continuity plans • Review compliance and sustainability risks • Review the Company’s risk philosophy and assess the extent of risk, that the Company may accept in pursuit of stakeholder value • Review the extent to which management has established effective enterprise risk management • Review effectiveness of risk management processes • Review the Company’s portfolio of risk vis-a-vis its risk appetite to ensure that risk exposures are consistent with overall appetite

Level	Key Roles & Responsibilities
	<p>for risk</p> <ul style="list-style-type: none"> • Review key risk indicators and management response thereto • Review the appointment, removal and terms of remuneration of the Chief Risk Officer (“CRO”) (if any) • Review issues raised by External Audit or Internal Audit that impact the risk management framework • Review and make recommendations to the Board on draft statutory statements covering governance and risk management issues in accordance with the requirements of the regulations • 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 • Approve the risk assessment criteria as detailed in the ERM Handbook • Promotes risk culture that aligns with the maturity of the Company
Chief Risk Officer	<ul style="list-style-type: none"> • Assisting Risk Management Committee in fulfilling their respective risk oversight responsibilities • Monitor compliance with this policy • Providing overall leadership to ERM process in line with directions of the Board of Directors and Audit Committee • Develop, implement and maintain Company’s risk management strategy • Develop, enhance, implement, maintain appropriate risk management policies, procedures and systems • Establishing procedures and timelines for various risk management activities • Providing necessary information and feedback to facilitate definition of risk appetite at the business line/ function, entity, and organization level • Liaising with Risk Management Committee at various levels for deploying the ERM process • Facilitating risk identification, evaluation, prioritization and consolidation • Assisting the respective Business Units, Corporate Functions in the identification of risk owners for each risk • Report to the RMC and the Board on compliance with policy • Developing, implementing and monitoring systems, management of policies and procedures relevant to the business, including facilitating regular review to maintain the risk register.

Level	Key Roles & Responsibilities
	<ul style="list-style-type: none"> • Ensure that relevant and emerging risk information is reported, escalated or cascaded, as the case may be, in a timely manner, to the Risk Management Committee • Promoting risk management culture through trainings, reporting and other internal communications • Enable development and maintenance of the necessary risk management competencies • Leverages the Company's information and technology systems to support enterprise risk management
Divisional Risk Management Committee (Coordination Committee)	<ul style="list-style-type: none"> • Identify and assess risks and changes in the risk profile • Identify and assess emerging risks • Execute directives from CRO • Implement risk mitigation plans for identified risks • Enhance awareness of risks within respective units, divisions and functions • Ensure risk documentation and monitor risk mitigation plans • Recommend training programs for staff with specific risk management responsibilities • Perform half yearly review of risk register • Assist risk owners to identify, analyze and mitigate risks • Escalate issues requiring policy approvals to CRO
Risk Coordinator	<ul style="list-style-type: none"> • Coordinate the risk management activities for respective division/ function in accordance with the risk management policy and directives of Coordination Committee • Coordinate between the CRO and Risk Owners • Report to the Coordination Committee on risk management activities. • Ensure that the required documentation is maintained and the required sign offs have been obtained
Risk Owners	<ul style="list-style-type: none"> • Identify and assess the risks • Reassess risks on a periodic basis • Prepare risk register and document mitigation plan and risk profile for approval from Coordination Committee • Manage risk by implementing mitigation plans and report on risk management activities to the Coordination Committee through the Risk Coordinator • Escalate risks to Coordination Committee through the Risk Coordinator on a need basis
Internal Audit	<ul style="list-style-type: none"> • Provide independent assurance of the risk management system and the processes supporting it

Level	Key Roles & Responsibilities
	<ul style="list-style-type: none"> • Review the overall effectiveness of the risk management measures and controls • Align internal audit plans to risk profiles to ensure that risk management activities for all key risks are covered as a part of the internal audit process • Internal Audit shall share the respective audit reports with the ERM function on a need basis. The ERM function may use this information as an input for risk treatment plans

9 Risk Management Framework

ERM Framework



Based on ISO & COSO

10 Risk Management Process

The Risk Management process comprises of the following phases as hereunder:

10.1 Objective Identification

Before identifying the risks, it is important to establish the context by clarifying the objectives. This can be the overall strategy of the Company, the outcomes, the outputs, the annual operation plan or specific expansion plan.

10.2 Risk Identification

Risk identification consists of determining the risks that are likely to affect SMIORE and documenting their characteristics.

10.3 Risk Categorization

This comprises of classifying risks under the following categories, based on their root causes:

- a) **Strategic Risks**, relating to the Company's business model, industry trend, market, competition, technology, investment evaluation in new product, resources, political stability and related matters.
- b) **Financial Risks**, which include events that on materializing will create financial obligations on the Company or will impact the profitability of the Company such as change in interest rate, cost over-run consequent to delays in project implementation, commodity pricing changes, cash flow constraints and so on. Financial risk relating to treasury, investment and hedging has to be read in conjunction with treasury and hedging policy of the Company.
- c) **Operations Risks**, which arise due to difficulty in meeting production targets, caused in turn by improper sales planning, non-availability of raw materials, contractual obligations, improper equipment planning including non-availability of spares on time, breakdown of machinery, fraud risks etc.
- d) **Environment Health & Safety Risks**, that arise due to non-compliance to safety standards of the Company which may result in loss of human life or property.
- e) **Compliance and Legal Risks**, that arise due to violation of/ or non-compliance with statutory requirements, legislative amendments, judicial decisions, contractual disputes, public interest litigations, environmental regulations etc.
- f) **Reputational Risks**, which are events that on materializing will impact the reputation of the Company.
- g) **Social Risk**, such as local obstructions, constraints in manpower or land availability etc.
- h) **Cyber Risks**, which are potential threats as a result of attacks on information systems.
- i) **Technology Risk**, which are risks associated with technology absorption by the Company.

10.4 Risk Analysis and Prioritization

Risks are assessed based on the following criteria:

- Impact: The potential damage a risk event could cause
- Likelihood: The possibility of a risk occurring
- Velocity: The expected speed with which risks will affect operations, once an event occurs

The following scale shall be used to determine the level of risk:

Likelihood		Impact	
Level	Descriptors	Level	Descriptors
5	Almost Certain	5	Severe
4	Likely	4	Major
3	Possible	3	Moderate
2	Unlikely	2	Minor
1	Rare	1	Negligible

Risk shall be rated on the basis of quantitative (E.g., financial consequence) or qualitative parameters (E.g., operational effectiveness, reputation)

Risk rating criteria shall be proposed by the Chief Risk Officer to the Risk Management Committee for further inputs. Approval to the same shall be given by the Board of Directors.

Based on the combined score on impact and likelihood, risks shall be classified into various Zones as hereunder and accordingly risks will be prioritized, reported & monitored.

- **Red Zone or ‘High’ risks**, that require immediate action (Average score greater than 10). They are reported to the RMC, AC and the Board (as applicable)
- **Yellow Zone or ‘Medium’ risks** where the focus is to further enhance existing controls. (Average score including and between 4 and 10). They are reported and monitored by the Chief Risk Officer and the Divisional Risk Management Committee
- **Green Zone or ‘Low’ risks**, which are considered to be under control. (Average score less than or equal to 3). They are managed by the Divisional Risk Management Committee and respective risk owners

Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16 ●	20
Possible (3)	3 ■	6	9 ▲	12	15
Unlikely (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5
Likelihood / Impact	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)

▲ High velocity

■ Medium velocity

● Low velocity

Notes:

- Velocity will be assessed qualitatively and will be represented in the Risk Heat Map as per the depiction above.
- Risks which fall in the 'Yellow' zone but carry a high velocity will be considered for reporting to RMC, AC and the Board based on their qualitative assessment.

10.5 Response to and Mitigation of Risk

Risk mitigation responses may include: -

- Accepting the risk level within established criteria;
- Transferring the risk to other parties viz. insurance;
- Avoiding the risk by hedging or adopting safer practices or policies; and
- Reducing the likelihood of occurrence and/ or consequence of a risk event.

10.6 Risk Documentation and Reporting

All risks shall be documented in the risk register, which shall capture all risks, external and internal, its consequences, impact, risk scores and the mitigation plan in a systematic manner.

A risk review involves re-examination of all risks recorded in the risk register and the revalidation of risk profiles. The risk register shall be reviewed, assessed and updated on a periodic basis.

All risks related to fraud, corruption and anti-competition shall be reported promptly, independently of the amount and the probability of occurrence.

10.7 Training and awareness

The Board of Directors to oversee the effectiveness of risk management trainings. The CRO shall ensure that:

- All employees (including new joiners) are trained in the risk management policy and procedure as required by their roles and responsibilities.
- Refresher training is provided on an annual basis to all the employees.
- Emphasis is given to training on risk management and improvement of process controls.
- All staff understand the Company's approach to risk management.
- All staff understand the benefits of risk management in their respective areas and applies the risk management principles in day-to-day operations.

11 Risk Appetite

Risk appetite is the amount of risk that the Company is willing to pursue or retain in pursuit of its objectives.

The risk appetite statements are defined under three key parameters:

Financial parameters which provide the threshold in terms of

- Impact on annual budgeted revenue
- Impact on annual budgeted profit
- Impact on project Internal Rate of Return (variation from cost of capital)
- Impact on project NPV (variation from projected cash flows)
- Impact on budgeted costs/ cost to completion in case of projects in construction stage.

Reputation parameters with respect to specific stakeholders

- Investors, analysts, lenders and rating agencies
- Key customers
- Key vendors/ alliance partners
- Employees
- Media/general public

Other qualitative parameters have been articulated that set out the appetite with regard to

- Environment, Health and Safety
- Business disruption/ project delays
- Legal issues
- Position with the regulator

Risk appetite shall form an integral part of the risk management framework to demonstrate common understanding of the same, and to consistently measure risks across the organization.

12 ERM Calendar

#	Activities	Responsibility	Frequency
1	Assessment and approval of Company's Risk Appetite (including risk assessment parameters)	RMC	Once in two years
2	Reevaluate top enterprise risks of strategic impact	RMC & CRO	Annual
3	Review, update (where necessary) and communicate the ERM policy	RMC & CRO	Once in two years
4	Inputs on risk from CRO in preparation of budget & Risk identification (new risk)/ Risk Validation (existing risk) based on the budget	CRO & Business	Annual

#	Activities	Responsibility	Frequency
5	Risk identification based on ‘Signals of Change’ (Risk Drivers)	CRO	Ongoing
6	Inputs to Audit Committee for consideration in development of internal audit plan	CRO	Annual
7	Risk Assessment for calculating ‘Gross or Inherent Risk’ and ‘Residual Risk’	CRO	Ongoing
8	Review and update the Risk Register	CRO	Ongoing
9	Monitor and update/ create Risk Profiles (including mitigation plans)	CRO	Ongoing
10	Monitor Risk Indicators agreed with the Risk/ Mitigation Owners	CRO	Quarterly
11	Update to RMC on material loss events	CRO	Need based
12	Risk Reporting to the RMC	CRO	Half-Yearly
13	Portfolio view of Risks to BOD	CRO	Annual

13 Risk Management Integration with Other Policies

All other risk management policies and procedures within the Company will comply with the requirements of this Enterprise Risk Management philosophy and risk appetite of the Company.

14 Disclosure

The Risk Management Policy shall be disclosed in the Annual Report and on the website of the Company i.e., at www.sandurgroup.com

15 Review/ Amendment of the Policy:

The Board shall review this Policy at least once in two years. This policy, including definition and other provisions of the policy shall stand automatically amended in the event of any relevant regulatory amendments, clarifications etc. in the applicable laws, rules and regulations.

In case of any amendments, clarifications, circulars, notifications, etc., issued by the relevant authorities, not being consistent with the provisions of this policy, such amendments, clarifications, circulars, etc. shall prevail over the provisions of this policy.

16 Policy Compliance:

No exceptions to this policy are authorized without written consent from the Chief Risk Officer. Any evidence of non-compliance with this policy will be documented and reported in writing to the Chief Risk Officer so that the root cause may be identified, and the proper corrective action may be taken.