Risk Management Policy

(Version 3.2)

Document properties:

Version	3.2		
Changes made	Policy updated and incorporated elements pertaining to- Risk Management Principles as per ISO 31000, Composition of Risk Council, Risk Rating criteria, Management Review Committee at Plants and other aspects. Basis the inputs of RMC in Aug-23, composition, quorum and meeting frequency of RMC and Risk council defined on page numbers- 12, 13, 14.		
Review Frequency	Annual and need based		
Approval	Prepared by	Reviewed by	Approved by
	Risk Management Department	CFO	Risk Management Committee (dated 30th Oct 2023)
Update Effective Date	Version- 3.2- October– 2023 Previous version- 3.1 tabled in RMC August- 2023		

Table of Contents

1. Overview 3
1.1 Introduction 3
1.2 Objectives 4
1.3 Definitions 4
1.4 Principles of Risk Management 5
1.5 Risk Management concepts 6
2. Risk Management Framework 8
2.1 Risk Management Process 8
2.2 Risk Management Governance Structure 11
2.3 Risk Management Committee 12
2.4 Roles and Responsibilities of Stakeholders 12
3 Approach and Tools Used for Risk Management 16
3.1 FMEA (Failure Mode and Effect Analysis) 16
3.2 ISO Standards 18
4 Risks Review and Monitoring 19

1. Overview

1.1 Introduction

Statement on Risk Management

The JSP Group recognises that managing risk effectively is critical to achieve the business objectives. Every Business and various Functions are required to review their environment, state clear objectives and:

- Identify risks to the achievement of those objectives;
- Assess the impact and likelihood of the risks;
- Implement effective actions designed to:

  - ✓ Achieve business objectives;
  - ✓ Safeguard company assets from inappropriate use or loss;
  - ✓ Facilitate economic, effective, efficient and safe operations;
  - ✓ Enable Compliance with the applicable Laws, regulations and Company policies

Every Business and Function should monitor, communicate and report changes in the risk environment and the effectiveness of actions taken to manage the identified risks on an ongoing basis.

Managing Risk Effectively

Risk is defined as a potential future event that may affect the achievement of objectives. This includes both "upside" and "downside" risks. Effective risk management increases the value from business decisions, because conscious choices are made in relation to risks that may have an impact on business decisions.

The Statement on Risk Management applies to all Businesses, Functions, and Business Units and to all activities that these entities undertake. This includes opportunity development, project execution and day-to-day operations. In general many people are involved in managing risk and risk management is an integral part of the Group's management activities (strategy, planning, execution, operation, monitoring and appraisal); it is not a separate activity. However, leadership teams at the Business, Function and Business Unit level are required to manage significant risks in a systematic manner and in line with the guidance in this document.

1.2 Objectives

Risk Management is ingrained in the DNA of the company and has become an integral part of the business decision making. This Risk management policy aims at formalizing the process of identification and prioritization of the risks to formulate relevant mitigation plans.

The objectives of Risk management at JSP are to:

- Identify the risks based on the internal and external factors affecting the organization
- Better understand and prioritize the risk profile which may have adverse impact on the organization and continuity of business.
- Formulate relevant mitigation plans and monitoring the same for prioritized risks to better manage uncertainties

1.3 Definitions

Enterprise Risk Management - Enterprise Risk Management (ERM) is the systematic approach to identify and manage all key risks in an organization, in order to protect and enhance value

Risk – Risk is an uncertain event or condition that may have a negative effect on business goals

Risk Management – A structured, consistent and continuous process for identifying, assessing, prioritizing and developing mitigation plans for the relevant risks

Risk Register – Compendium of all risks finalized and detailed with risk definition, risk mitigation and risk contingency plans

Risk Prioritization – The process of prioritizing risks based on risk scores

Risk Score – The combined product of Severity, Occurrence and Detection is risk score

Risk Appetite Statement - "Risk appetite" is a broad description of the amount and types of risk an organization is willing to accept to achieve its objectives

1.4 Principles of Risk Management

As per ISO 31000, for effective risk management an organization should comply with the under mentioned principles. JSP uses the following principles and has adopted ISO and FMEA approach for overall Risk Management.

a) Integrated- Risk management is an integral part of all organizational processes. It is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes. Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

b) Structured and comprehensive- Risk management is systematic, uses structured and timely approach and contributes to efficiency and to consistent and reliable results.

c) Best Available information and addresses uncertainty- Risk management is based on the best available information, the inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation and expert judgement. Risk management explicitly takes account of uncertainty, the nature of that uncertainty and how it can be addressed.

d) Customized- Risk management is tailored and aligned with the organization's context and risk profile.

e) Inclusive- Risk management is transparent and inclusive and requires appropriate involvement of stakeholders and decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

f) Dynamic- Risk management is dynamic and responsive to change and continually senses and responds to change. As external and internal events occur, monitoring and review of risks take place and changes are made in plans wherever required.

g) Continual Improvement- Risk management facilitates continual improvement of the organization and suitable strategies are implemented to improve the Risk Management maturity for continuous improvement in the organization.

1.5 Risk Management concepts

1.5.1. Risk and Event

A. Risk
Simply stated risk is the possibility that an event will occur and adversely affect the achievement of objectives. Risks can be thought of as threats, uncertainty or lost opportunity

B. Event
An Event in the context of ERM is defined as an incident or occurrence from internal or external sources that affects achievement of JSP's objectives. Such "Events" may lead to one or more risks

1.5.2. Inherent Risk vs. Residual Risk
Risks need to be assessed to form an appropriate response. Assessment is done first at an inherent level and then at a residual level

A. Inherent Risk
Inherent risk is defined as the risk to an entity in the absence of any mitigating controls. All business activities have risks attached to them, whether these risks are caused by external or internal factors. These risks (in absence of any mitigating controls) are also referred to as "gross risks"

B. Residual Risk
Inherent risks may be controlled by introducing mitigating action plans. *The remaining likelihood and impact of a particular risk after management has taken action plans by way of instituting controls to alter the risk's likelihood or impact is called as residual risk.*
Where JSP has implemented effective controls to mitigate risks, the quantum of residual risks need to be monitored. Some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities

1.5.3. Business Risk vs. Operational Risk

A. Business Risk

Business risk is the risk that results from the decisions about the products and services offered by entity. When an entity decides to develop and market a particular product, there's a risk that the product won't work or that marketing campaign may fail. Other business risks include changes in the cost of raw materials and other components and managing technological developments that affect sales or manufacturing

B. Operational Risk

Operational risk may exist in the way in which entity carries out the decisions. Operational risk rises from the entity's internal decision-making and practices

1.5.4. Benefits of Risk Management

Risk management is an important aspect of any business, as risks are an integral part of business. Risk management helps organizations to manage risk within their risk appetite. Effective Risk management provides reasonable assurance regarding the achievement of the key organizational objectives in four broad categories: Strategic, Operations, Financial and Compliance. If an organisation has an effective Risk Management system, it helps in the following ways:

- Link growth, risk and returns - Risk management enhances the capacity to identify events, assess risks, set risk tolerances consistent with growth and return objectives;
- Rationalise resources - Deploy resources more effectively, thereby reducing overall capital requirements and improving capital allocations;
- Exploit opportunities - Identify and take advantage of positive events quickly and efficiently;
- Reduce operational surprises and losses - Recognise potential adverse events, assess risks and establish responses, thereby reducing surprises and related costs or losses;
- Report with greater confidence - Prepare internal and external insights that are reliable, timely and relevant; and satisfy legal and regulatory requirements. Ensure compliance with legal and regulatory requirements and identify risks of non-compliance

1.5.5. Limitations of Risk Management

Risk Management Framework, no matter how well designed and operated, does not guarantee achievement of all the entity's objectives, nor does it provide full assurance against material misstatements, loss or fraud, human errors or misjudgement in decision making or violation of regulations.

2. Risk Management Framework

The Risk Management Framework outlines the series of activities and enablers that the Company deploys to identify, prioritize and manage key risks including financial, operational, sustainability, information and cyber security risks.

2.1 Risk Management Process

A. State Clear Objectives

In the planning phase of any activity, realistic and measurable objectives are defined in the context of the relevant business environment. For a Business Unit these objectives are set during the business planning process. For a new business opportunity the objectives may be set during the identification and assessment phases of the opportunity realisation process and these may be subsequently refined at the time a mandate to negotiate is sought. At an individual level, objectives are set as part of the annual Goals and Performance Appraisal process.

B. Identification of Risks

The identification of risks can only have value or meaning when explicitly linked to the objectives. Different approaches can be taken to identify risks and the approach taken will depend on the size and complexity of the business/operation or the opportunity/project and the volatility of the risk environment.

Sources of risk may include economic, political, commercial, technical, financial and operational factors.

The identification of risks may result in a long list, but these all may not need to be monitored by management. Many of the risks are simply managed as part of day-to-day management, some risks may need to be combined because they address the same underlying issue and some may be managed at a different level in the organisation (e.g. at Operational level rather than at Business Unit level).

Respective risk owners are required to identify the applicable risks considering the business objectives and the environmental factors. Risk management exercise is to be carried out on an annual basis and the review of the key risks to be done on quarterly basis.

C. Assess Impact and Likelihood of Risks

The impact needs to take into account the immediate consequences of a risk materialising and also the knock-on effects.

Not all risks can be quantified. For some types of risk, for example risk to reputation, a qualitative assessment may be required. The assessment of likelihood needs to take into account the track record in managing the risk. For example, if the track record of an operating unit in credit-management is bad, then there is a higher likelihood of a credit default occurrence.

An assessment of the risk exposure without any actions in place is referred to as the gross assessment of the risk. The residual risk is defined as the risk that remains after taking into consideration the implemented actions.

D. Implement Effective Actions and Treatment of Risk

Risk assessment assists in allocating resources and prioritisation of actions, based on a comprehensive picture of all significant risks in the context of the objectives of the relevant entity.

Three generic actions can be taken to manage various risks:
1. Accept and control the risk: Accept the risk and put in place appropriate controls (preventative and detective) to manage the risk to maximise value.

2. Transfer and/or share risk: Some risks are transferred (for example to an insurance company) or shared (for example with contractors or joint venture partners).

3. Terminate or forego activity: Risks are avoided, for instance by stopping an activity or withdrawing from a country or market. Some risks are terminated in part through sale or divestment.

Generally, risks are retained and managed when an entity (e.g. Business, Function or Business Unit) has the capability to manage it better than others and is sufficiently rewarded for that. Alternatively, risk is transferred or shared when others are better able to manage the risk at an acceptable cost.

An important element in risk management is to evaluate the cost of transferring the risk and what opportunities are foregone with the transfer of the risk. An example of transferring risk at a fixed price is the purchase of insurance to cover physical damage to assets. The impact of the actions being taken and/or changes in the risk environment will change the acceptability of the risk.

E. Communicating and Monitoring Risks

Changing business conditions and decisions made in the course of running the business will continuously alter the risk profile of an entity. This makes it important to have frequent and explicit conversations about risk, in order to maintain continued awareness of key risks which are significant.

It also requires transparent communication of significant risk to decision makers so that decisions are made with full understanding of the risks and opportunities involved and how these will be managed. The respective Business, Function or Business Unit considers the risks and adjusts plans and the allocation of resources. In order to facilitate this process, Businesses and Functions appoint risk owners for each risk.

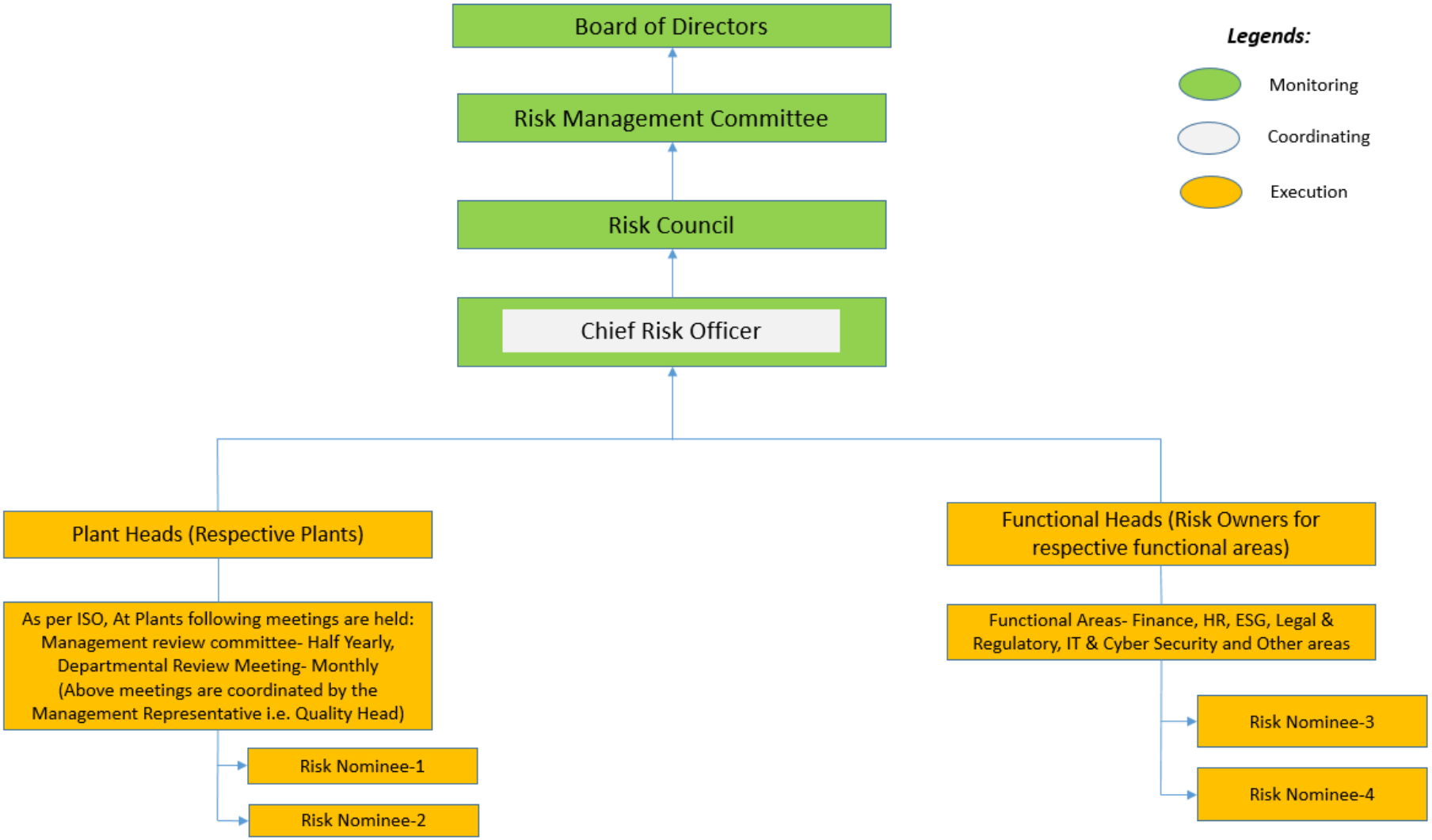
The respective Plant Heads are risk owners for the corresponding plants.
The respective corporate Functional Heads are risk owners for their respective domain area.

Risk owners are responsible for ensuring a clear definition and assessment of the risk is maintained and for considering the effectiveness of the existing actions to manage the risk. At the Group level the Risk Management Committee reviews the risks that may impact the Group's objectives.

F. Report Risks

The leadership teams of the Business, Functions and Business Units are required to review and report their risks on a quarterly basis. This facilitates aggregation of risks at the entity level.

2.2 Risk Management Governance Structure



2.3 Risk Management Committee

A. Purpose

The purpose of the Risk Management Committee (RMC) shall be to assist the Board of Directors (Board) to fulfil its responsibility of overseeing the Company's key risks, including strategic, operational, financial, sustainability, information, cyber security and any other risks, as deemed necessary, as well as the guidelines, policies and processes for monitoring and mitigating such risks.

The responsibility of risk assessment and risk management shall be the responsibility of the Company's management. The RMC shall have an oversight role.

B. Structure

RMC shall be appointed by and will serve at the discretion of the Board. The RMC shall have minimum three members with majority of them being members of the Board of Directors (BOD), including at least one independent director.

The Chairperson of the RMC shall be a member of the Board.

C. Meeting and Quorum

RMC shall meet once in a quarter. The 50% members of the committee shall be an independent directors including Chairman of the committee. The quorum for the meeting of RMC shall be either two members or 1/3 of members of committee, whichever is higher.

2.4 Roles and Responsibilities of Stakeholders

Board of Directors

The responsibility of Board of Directors (Board) shall be to oversee that:

- a suitable framework for managing risks has been put in place by the Company

- Framework has been effectively deployed by the Executive Management of the Company
- To appoint and define the roles and responsibilities of Risk Management Committee (RMC)
- To review performance of the RMC periodically

The Board has delegated the task of overseeing the deployment of the risk management framework to the RMC. On a periodic basis, a formal report on risks that matter, shall be submitted to the Board.

Risk Management Committee (RMC)

Key responsibility of RMC shall be to:

- Evaluate the operation of risk management program
- Approve risk appetite
- Review results of risk assessment prepared by the executive management
- Monitor results of risk mitigation plans

If there is a Committee of the Board focusing on the subject matter of an item that appears on the Risk Heat Map, then the review of that specific item should be undertaken by that Committee itself. For instance: Environment, Social and Governance (ESG) Risk to be reviewed and overseen by "Health, Safety, CSR, Sustainability and Environment Committee".

Risk Council (RC)

Risk Council shall have nominated members comprising of Plants leadership, Head Legal, CFO and others members will be joining as invitees wherever required.

The CFO shall be the chairman of the Risk Council. The CRO to ensure that RC meetings are conducted every quarter. RC shall meet once in a quarter. The quorum for the meeting of RC shall be 3 or more members present in the meeting.

Key responsibility of Risk Council shall be to:

- Review the work done on risk management areas and provide inputs on further strengthening the overall risk management for the enterprise
- Assisting the Risk Management Committee (RMC) in overseeing the company's key risks
- Review Risk Management program and mitigation actions on quarterly basis
- Review the risk appetite matrix (Severity /Occurrence /Detection scale) of the key risks at each quarter

Chief Risk Officer (CRO)

The responsibility of CRO shall be to:

- develop, enhance and implement the risk management policy, procedures and framework
- work with risk owners to facilitate that the risk management systems and processes are implemented
- develop monitoring mechanism for compliance to risk management policy
- collate and provide update on risk mitigation plan to the RMC on periodic basis

Management Review Committee (MRC) at Plants as per ISO standards

MRC at plants shall have nominated members comprising of Chairman of committee (i.e. Plant Head), Management representative (i.e. Plant Quality Head), Member Secretary, various HODs and Representative from other departments as needed may also attend the meeting. **The management review shall be carried out on half yearly basis**.

The responsibility of Management Review committee at plants shall be to:

- Review status of actions from previous management review
- Internal/ External audit findings- Status of Corrective and Preventive actions
- Scope of improvement through process monitoring findings or customer feedback
- Review various Trends- Customer complaints, Non-conformity in finished goods, Environmental monitoring results
- Status and reason for any shortfall in 'QSHE' (Quality standard for Health and Environment) objective, Environment programmes and OH&S programmes

- Status of corrective actions- Complaints and their resolution for interested parties, Accidents/ Emergency situation & the corrective and preventive actions initiated to prevent their recurrence
- Review the changes in Quality policy, Environment Policy and Safety & Occupational Health Policy and any major change in the system
- Review the present status and any corrective actions for any non- compliance
- Review the hazard identification and Risk assessment as per system procedures

Each Department to carry out Monthly Department Management Review (DMR) meeting at plant.

Agenda for Plant level Management Review Meeting:

- Status of actions from previous management reviews
- Changes affecting IMS Implementation
- Review of performance and effectiveness of management systems
- Any other specific points

Business heads / Functional heads / Risk Owners

The responsibility of Business heads / Functional heads / Risk owners shall be to:

- identify and evaluate the significant risks for their respective areas
- manage the risks for the respective locations and process areas
- develop and ensure implementation of risk mitigation plan including systems and processes for internal control of identified risks
- have periodic review and monitoring of applicable Risks and Mitigation actions and reporting thereof quarterly

Risk Nominee

- Risk nominee shall be a person nominated by the Business heads / Functional heads / Risk owners to take lead in risk management for respective department / functions
- The responsibility of risk nominee shall be to

- implement the agreed mitigation plans
- provide feedback on efficacy of risk management systems and processes
- review the risk and mitigation plans on a regular basis
- identify deficiencies in controls
- escalate the matter where the risk is increasing

3 Approach and Tools Used for Risk Management

Two tools are used to assess and mitigate the risks associated with the organization i.e. FMEA (Failure mode and effect analysis approach) and ISO approach.

3.1 FMEA (Failure Mode and Effect Analysis)

FMEA is systematic and comprehensive approach of risk management to identify and analyse potential effects of failure in product or process. It can be used as a tool for risk assessment within the ISO framework. FMEA is conducted by review of the various components of a product or process and identify potential failure modes, effects and causes. Then the likelihood and severity of each failure mode and potential mitigation plans are identified.

At JSP, we deploy FMEA tool to identify key risks applicable at various levels and in different functions or operations.

Various risks are identified along with potential failure modes i.e. what could go wrong and the Severity, Occurrence, Detection scores are assigned to them on a scale of 1 to 10. Further, Risk Priority Numbers (RPN score) are assigned to various risks which facilitate prioritizing the key risks and the mitigating actions required. RPN score can range from 1 to 1000.

RPN Score Matrix:

RPN Range (Severity X Occurrence X Detection)	Level	Meaning
>301-1000	Red	Critical - Major contributor to the identified problem - Abnormality Detection System needs to be introduced/ strengthened
>101-300	Yellow	Alarm - Medium contributor to the identified problem - Abnormality Detection System needs to be strengthened
1-100	Green	Normal - Least contributor to the identified problem - To continue with the current Controls of Prevention/ Detection

Basis of Risks Ranking and Colour category:

Criteria – based on RPN Score and residual risk	Red	Yellow	Green
RPN Score	>301-1000	>101-300	1-100
Risk Significance or Impact (Gross Risk)	High	High/ Medium	High/ Medium/ Low
Mitigating Actions or initiatives	Yet to be implemented or partially implemented	Implemented but needs strengthening	Implemented
Residual Risk (Net Risk)	High	Medium	Low

Risk Appetite - JSP uses FMEA process to evaluate, assess and mitigate risks

Any risk with Risk Priority RPN Score of 100 or more needs to be monitored and addressed to mitigate the same.

All Units have to target that overall risk RPN score should eventually come to less than 100.

The requisite remedial actions should continue and risk review process to be repeated every quarter till the underlying risks are brought at an acceptable level i.e. RPN below 100.

Wherever severity, occurrence level is high, risk owners need to focus on detection measures so that overall RPN score is brought down to less than 100.

Implementation - All the JSP units are responsible for the implementation and compliance with this policy.

Each business unit needs to maintain a Risk Register of the business risks it faces in its day-to-day operations and to ensure that the control framework is in place to mitigate risks. These Registers should consider risks from within the company and external factors and should be reviewed periodically. Risk Registers are also updated where necessary when there are critical changes in policies, structures or environment and responses to incidents.

3.2 ISO Standards

ISO is a family of standards that provide guidelines and best practices for various aspects of risk management. Presently, organization is following ISO- 9001 (Quality management system), ISO- 14001 (Environmental management), ISO- 45001 (Occupational health and safety management) and ISO-31000 (overall Risk Management) as an Integrated management tool to identify and mitigate the risks.

JSP deploys ISO Integrated Management System (IMS) at various plants to monitor various processes and implement best in class quality of products and services.

A. ISO 9001- It provides the QMS requirements to be implemented for creation of various policies, processes, and procedures necessary to provide products and services that meet customer and regulatory needs and improve customer satisfaction. This standard is an internationally recognized **Quality Management System (QMS)** standard that can benefit any size organization and is a powerful business improvement tool. The adoption of a quality management system is a strategic decision for an organization that can help to improve its overall performance and provide sustainable development to organization.

B. ISO 14001- This is a guide on what needs to be done to implement an **Environmental management system (EMS)**. It comprises of policies, processes, plans, practices and records that define the rules governing how company interacts with the environment. ISO 14001 requirements provide a framework and guidelines for creating EMS in the organization.

C. ISO 45001- ISO 45001 is **Occupational Health & Safety (OH&S) management system** ISO standard. Its focus on risk prevention, innovation and continual improvement provides benefit to achieve improved organizational resilience. It allows organizations to tailor occupational health and safety management systems to their workplace more effectively.

4 Risks Review and Monitoring

All Functions and Business Units have to deploy FMEA process for identification, assessment and mitigation plans for identified risks.

- The respective Plant Heads are risk owners for the corresponding plants. **Respective Plant Heads to review the applicable risks for the respective plant / locations**
- The respective corporate Functional Heads are risk owners for their respective domain area. **Respective Functional Head to review the risks pertaining to the corresponding functions / process areas**
- **The respective Risk owners are responsible to review, monitor and report on the applicable risks and requisite mitigation actions quarterly.**
- **The key major risks need to be reviewed by Business Heads, Functional Heads, CXOs quarterly, and by the Risk Council at the management level, and by the Risk Management Committee as part of the periodic review Meetings of the Board.**

A. ISO review process at Plants:

Risk Register at Plants is maintained under ISO 9001, ISO 14001 and ISO 45001 taking into considerations the aspects of ISO 31000 for the following Departments:

- **Core Processes** – Blast Furnace, Coke Oven, DRI, Plate Mill, SMS, Rail Mill, etc.
- **Service Department** – Contract cell, Purchase, Civil, Environment, Safety, Human Resources, Stores, etc.
- **Risk Review & Evaluation** done using IMS Review Methodology
- **ISO Checklist** Internal Audit for various areas done quarterly
- **Management Review Meeting** – Half yearly frequency at Unit Head Level
- **Departmental Management Review Meeting** – Monthly with respective HOD

- HODs at each Plants are **responsible for determining and managing the risks & opportunities and ensure the continual improvement** in their respective area

The applicable Quality and ISO teams at the plants and various locations are leveraged for driving the risk management program at the ground level.

B. Areas covered in ISO/IMS at JSP (further areas may be added based on requirement):

1. Blast Furnace
2. Coke Oven
3. Coal Washery
4. Central services
5. DRI
6. EPS
7. LDP
8. BSM
9. Oxygen plant
10. Power plant
11. PGP
12. Rail Mill
13. RMH
14. Steel Melting Shop
15. SAF
16. Sinter Plant
17. Civil
18. Plate Mill
19. Contact Cell
20. Human Resources
21. Information Technology
22. OH, Safety and Fire
23. Purchase
24. Marketing and logistics
25. Environmental management
26. Canteen
27. Stores
28. Technical Services
29. CSR