JINDAL SAW LTD.
TOTAL PIPE SOLUTIONS

Risk Management Policy

About Jindal SAW Limited

Jindal SAW Ltd. started operation in the year 1984, when it became the first company in India to manufacture Submerged Arc Welded (SAW) Pipes using the internationally acclaimed U-O-E technology.

Jindal SAW Ltd. is in a commanding position in India's tubular market, being the undisputed leader. With integrated facilities at multiple locations and an ever expanding market opportunity, Jindal SAW Ltd. has diversified from a single product company to a multi-product company, manufacturing large diameter submerged arc pipes and spiral pipes for the energy transportation sector; carbon, alloy and stainless steel seamless pipes and tubes manufactured by conical piercing process used for industrial applications; and Ductile iron (DI) pipes for water and wastewater transportation. Besides these, the Company also provides various value added products like pipe coatings, bends and connector castings to its clients.

Ensuring timely transportation of oil, gas and water, Jindal SAW helps residents and organizations in numerous cities function efficiently. The pipes produced by the Company are energy efficient, reduce dependence on fossil fuels, and help conserve natural resources like water.

There are four major business verticals:

- Large Diameter (LD) Pipes
- Ductile Iron (DI) Spun Pipes
- Seamless Tubes & Pipes
- Pellets

The Company has facilities at Samaghogha, Pragpar and Nana Kapaya in Gujrat; Nashik in Maharashtra; Bellary in Karnataka; Kosi Kalan in Uttar Pradesh and Bhilwara in Rajasthan, with Corporate Office in Delhi.

Contents

1. Introduction :

1.1 Objectives

Risk is an inherent aspect of the dynamic business environment. Risk Management Policy helps organizations to put in place effective frameworks for taking informed decisions about risks. To minimize the adverse consequence of risks on business objectives the Company has framed this Risk Management Policy. The guidance provides a route map for risk management, bringing together policy and guidance from Board of Directors.

Importance of Risk Management

A certain amount of risk taking is inevitable if the organization is to achieve its objectives. Effective management of risk helps to manage innovation and improve performance by contributing to:

- Increased certainty and fewer surprises,
- Better service delivery,
- More effective management of change,
- More efficient use of resources,
- Better management at all levels through improved decision making,
- Reduced waste and fraud, and better value for money,
- Innovation,
- Management of contingent and maintenance activities.

1.2 Requirement as per Companies Act, 2013

Responsibility of the Board: As per Section 134 (n) of the Act, The Board of Directors' report must include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

Responsibility of the Audit Committee: As per Section 177 (4)(vii) of the Act, the 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 controls and risk management systems.

Responsibility of the Independent Directors: As per Schedule IV [Part II-(4)] of the Act, Independent directors should satisfy themselves that financial controls and the systems of risk management are robust and defensible.

1.3 Requirement of Clause 49 of the Listing Agreement

Responsibility of the Audit Committee: As per Clause II.D, The role of the audit committee shall include the reviewing of the company's financial and risk management policies.

Requirement for revised Clause 49(VI) (C): "The Company through its Board of Directors shall constitute a Risk Management Committee. The Board shall define the roles and responsibilities of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit. "

1.4 Definitions

Company: Means Jindal SAW Ltd.

Audit Committee: Committee of Board of Directors of the Company constituted under the provisions of the Companies Act, 2013 and the Listing agreement.

Board of Directors / Board : As per Section 2 of "The Companies Act, 2013", in relation to a Company, means the collective body of Directors of the Company.

RMP / Policy: Risk Management Policy

Risk*: 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.
- 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 customers and third parties.
- Knowledge Risks are associated with the management and protection of knowledge and information within the enterprise.

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

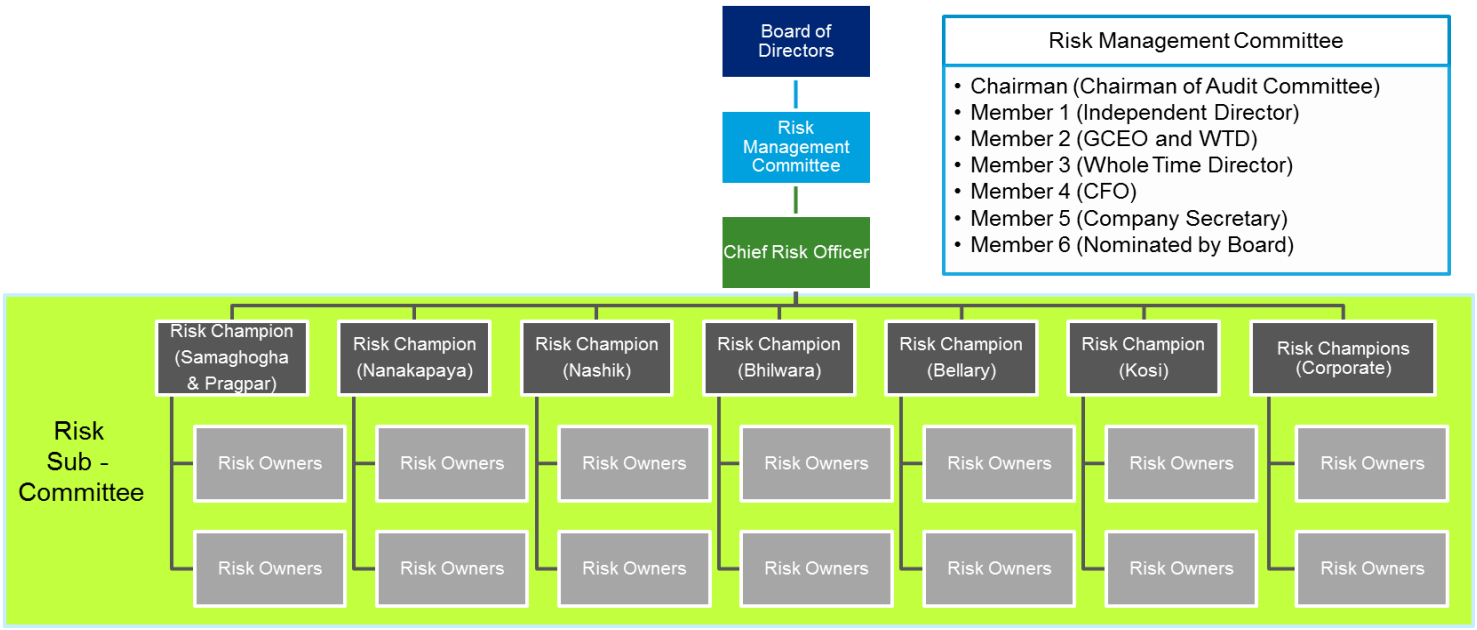
Inherent Risks : The risk management process focuses on areas of high inherent risk, with these documented in the Risk Register. Recent performance in delivering a core service that is below expectations or does not meet agreed targets should be considered an indicator of high inherent risk.

Residual Risks : Upon implementation of treatments there will still be a degree of residual (or remaining) risk, with the expectation that an unacceptable level of residual risk would remain only in exceptional circumstances.

Risk Appetite : Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value.

2. Risk Organization Structure

For successful implementation of risk management framework, it is essential to nominate senior management individuals to lead the risk management teams. Periodic workshops will be conducted to ensure awareness of the policy and the benefits of following them. This will ensure that risk management is fully embedded in management processes and consistently applied. Senior management involvement will ensure active review and monitoring of risks on a constructive 'no-blame' basis.



	Constitution	Roles and responsibilities	Accountable to
Risk Management Committee (RMC)	* Constituted with approval of Board; * There shall be 7 members: - Chairman of Audit Committee as Chairman of RMC, - an Independent Director, - Group Chief Executive Officer ("GCEO") and Whole Time Director ("WTD"), - Whole Time Director - Chief Finance Officer, - Company Secretary, - one more member nominated by the Board.	* To frame, implement and monitor the Risk Management Plan for the Company. * To ensure that the Risk Management Policy is being followed and effectively contributing to early identification of risks and proper mitigation process. * Will review and approve list of risk identified, risk treatment and control mechanism. * To lay down procedure to inform the Board members about the risk assessment and minimization procedure.	Board of Directors

Chief Risk Officer (CRO)	*CRO Shall be nominated by the RMC, * CRO shall be supported by Risk Sub Committee	*To coordinate meeting of RMC at least once in each quarter *To monitor the mitigation plan for the risks identified in the consolidated risk register and place it for review of Risk Management Committee in the meeting *To facilitate circulation of Agenda for the RMC meeting. *To attend all RMC meetings. *To facilitate maintenance of minutes of all RMC meetings. *All key risks identified shall be documented in the Consolidated Risk Register maintained by Chief Risk Officer *To propose periodic updates in risk management policy.	Board of Directors
Risk Sub Committee (RSC)	*Shall be formed at each location of operations viz. Corporate Office, Samaghogha (including Pragpar), Nanakapaya, Nashik, Bhilwara, Kosi and Bellary. *RSC(s), shall comprise of Risk Champion and Risk Owners.	*It will evaluate the risk and mitigation plan recommended by Risk Owners. *Risk Sub Committee to hold its meeting at least once every month starting from October, 2015. *It will direct Risk Owners for mitigating the risks identified. *Will draft risk analysis, risk treatment and control mechanism. *Risk Sub Committee will update risk register and communicate to CRO. *Risk Register should be updated by any new risk identified to be placed to RMC for approval.	Risk Management Committee
Risk Champion (RC)	*Respective Unit Heads/ Functional Heads will be Risk Champion for Unit RSC(s)/ Corporate RSC(s). *Whole Time Director/ Unit Head will also act as Risk Owner of different strategic risks which are not covered under the scope of various Departmental Heads at Corporate/ Unit level, respectively.		Risk Management Committee
Risk Owners	*Risk Owners shall be nominated by Risk Champions. *Each of the department shall be represented by a Risk Owner. List of Departments : 1. Production, 2. Maintenance, 3. Marketing, 4. Purchase, 5. Inventory and store, 6. Projects, 7. Accounts and Taxation, 8.Finance & Treasury, 9. Human Resource, 10. Scrap, 11. Corporate Strategy, 12. Statutory Compliance, 13. Environment Health and Safety, 14. Administration and Security, 15. Quality Control, 16. Corporate Communication, 17. Information Technology , 18. Internal Audit, 19. Dispatch and Warehouse	*The Risk Owner will be responsible for identification and mitigation of risk of their respective areas. *Risk Owner shall present the new risks identified along with proposed mitigation plan to Risk Sub Committee and Risk Champion for their approval. *Identify future risk, evaluate the critically of the risk and formulate the steps of mitigation. *To maintain and update register of their concerned areas, and communicate to RC.	Risk Champion

3. Risk Management Framework

3.1 Process

Risk management is a continuous process that is accomplished throughout the life cycle of a Company. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction.

Effective risk management depends on risk management planning; early identification & analyses of risks; early implementation of corrective actions; continuous monitoring & reassessment; communication, documentation, and coordination.

3.2 Steps in Risk Management

Risk management is a shared responsibility. The risk management process model includes the following key activities, performed on a continuous basis:

3.2.1 Risk Identification

This involves continuous identification of events that may have negative impact on the Company's ability to achieve goals. Processes have been identified by the Company and their key activities have been selected for the purpose of risk assessment. Identification of risks, risk events and their relationship are defined on the basis of discussion with the risk owners and secondary analysis of related data, previous internal audit reports, information from competition, market data, Government Policies, past occurrences of such events etc.

3.2.2 Risk Assessment

Risk assessment is the process of risk prioritization or profiling. Likelihood and Impact of risk events have to be assessed for the purpose of analyzing the criticality. The potential Impact may include:

- Financial loss;
- Non-compliance to regulations and applicable laws leading to imprisonment, fines, penalties etc.
- Loss of talent;
- Health, Safety and Environment related incidences;
- Business interruptions / closure;
- Loss of values, ethics and reputation.

The likelihood of occurrence of risk is rated based on number of past incidences in the industry, previous year audit observations, Government Policies, information from competition, market data, future trends or research available. For detailed likelihood ratings refer to Appendix 5.2.

Risk may be evaluated based on whether they are internal and external, controllable and non-controllable, inherent and residual.

3.2.3 Risk Analysis

Risk Analysis is to be conducted using a risk matrix for likelihood and Impact, taking the existing controls into consideration. Risk events assessed as “high” or “very high” may go into risk mitigation planning and implementation; low and medium risk to be tracked and monitored on a watch list.

The Risk Reporting Matrix below is typically used to determine the level of risks identified. A risk reporting matrix is matched with specific likelihood ratings and Impact ratings to a risk grade of low (green), medium (yellow), high (amber) or very high (red).

Consequences	Likelihood				
	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost certain
5 Very High					
4 High					
3 Medium					
2 Low					
1 Insignificant					

Risk Score = Business Impact x Likelihood	
more than 15	Very High
9 to 15	High
4 to 8	Medium
3 or less	Low

3.2.4 Risk Treatment - Mitigation

Risk mitigation options are considered in determining the suitable risk treatment strategy. For the risk mitigation steps, the cost benefit analysis needs to be evaluated. Action plans supporting the strategy are recorded in a risk register along with the timelines for implementation.

3.2.5 Control and Monitoring Mechanism

Risk management uses the output of a risk assessment and implements countermeasures to reduce the risks identified to an acceptable level. This policy provides a foundation for the development of an effective risk register, containing both the definitions and the guidance necessary for the process of assessing and mitigating risks identified within functions and associated processes.

In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated, such risk shall form part of consolidated risk register along with the business justification and their status shall be continuously monitored and periodically presented to Risk Management Committee and Audit Committee.

3.3. Board's responsibility statement

Board of Directors 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.

The Board of Directors of the Company, Audit Committee and Risk Management Committee shall periodically review and evaluate the risk management system of the Company, so that the Management controls the risks through risk management framework.

The Company has a control processes in place to help ensure that the information presented to senior management and the Board is both accurate and timely. The control processes include, among other things:

- Annual audit and interim review by the Company's external auditor;
- Planned review by internal auditors reviewing the effectiveness of internal processes, procedures and controls;
- Monthly review of financial performance compared to budget and forecast.

3.4. Internal Audit (IA)

The Audit Committee is responsible for approving the appointment of the internal auditor and approving the annual internal audit plan.

As per Section 138 (1) of the Companies Act, 2013, the Internal Auditor shall either be a chartered accountant or a cost accountant, or such other professional as may be decided by the Board to conduct internal audit of the functions and activities of the company.

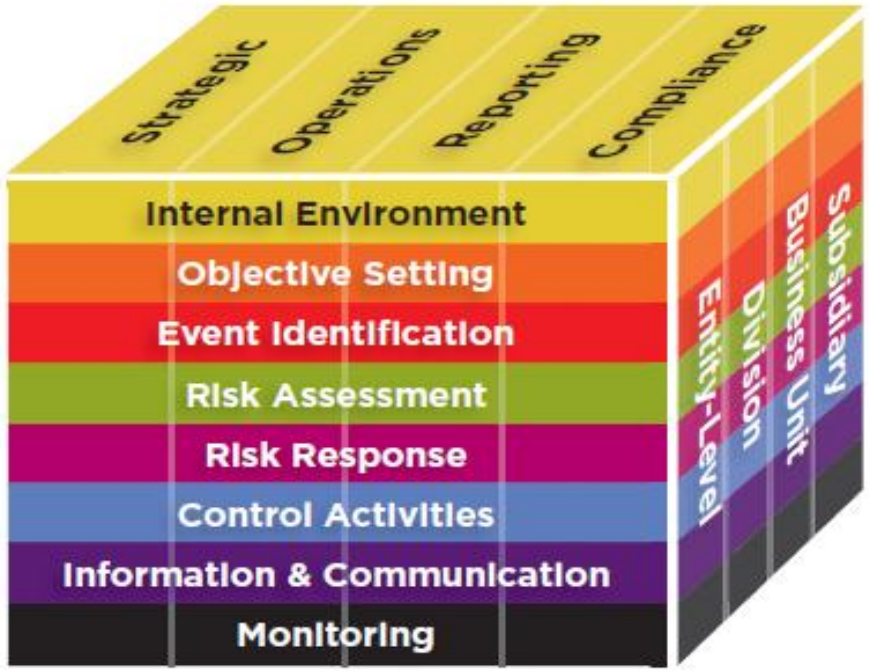
The GCEO in addition to their general and specific responsibilities, is responsible for the co-operation necessary to assist the Internal Auditor in carrying out internal audit.

Internal Audit function is independent of the external auditor and to ensure its independence, has direct access to the GCEO and Audit Committee.

Any deviations from the Company's policies identified through internal audits are reported to responsible authorities for action and to the GCEO & Audit Committee for information or further action.

4.1. COSO Guidelines (extract for reference)

COSO broadly defines enterprise risk management (ERM) as “a process, effected by an entity’s Board of Directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”



The COSO ERM framework is presented in the form of a three-dimensional matrix. The matrix includes four categories of objectives across the top – strategic, operations, reporting and compliance. There are eight components of enterprise risk management, which are further explained below. Finally, the entity, its divisions and business units are depicted as the third dimension of the matrix for applying the framework. As outlined by COSO, the framework provides eight components for use when evaluating ERM.

4.1.1. The Objective Dimension

This enterprise risk management framework is still geared to achieving an entity's objectives; however, the framework now includes four categories:

- Strategic: high-level goals, aligned with and supporting its mission
- Operations: effective and efficient use of its resources
- Reporting: reliability of reporting
- Compliance: compliance with applicable laws and regulations

4.1.2 The Framework Component Dimension

- **Internal Environment**: This component 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.
- **Objective-Setting**: Management sets strategic objectives, which provide a context for operational, reporting and compliance objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity, and are a precondition to event identification, risk assessment and risk response.
- **Event Identification**: Management identifies potential events that may positively or negatively affect an entity's ability to implement its strategy and achieve its objectives and performance goals. Potentially negative events represent risks that provide a context for assessing risk and alternative risk responses. Potentially positive events represent opportunities, which management channels back into the strategy and objective-setting processes.
- **Risk Assessment**: Management considers qualitative and quantitative methods to evaluate the likelihood and impact of potential events, individually or by category, which might affect the achievement of objectives over a given time horizon.
- **Risk Response**: Management considers alternative risk response options and their effect on risk likelihood and impact as well as the resulting costs versus benefits, with the goal of reducing residual risk to desired risk tolerances. Risk response planning drives policy development. It is also known as the Risk Management Policy, management may adopt different risk management strategies based on risk assessment, namely,
    - Tolerate/Accept the Risk: This strategy is adopted when impact of risk is minor. In this case risk is accepted as cost of mitigating the risk can be high. However, these risks are reviewed periodically to check their impact remains low else appropriate controls are used.
    - Terminate: In this case the activity, technology or task which involves risks is not used/conducted to eliminate the associated risk.
    - Transfer: In this approach the associated risks are shared with the trading partners and vendors etc. e.g. outsourcing IT services to IT service Providers who have better capabilities to manage IT related risks. Insurance is another example of sharing risks.
    - Treat: In this case, organizations use appropriate controls to treat the risks e.g. using an antivirus software is a control for risks related to virus.
    - Turn Back: This strategy is adopted when impact of risk is expected to be very low or chances of occurring risk are minimum in such cases management decide to ignore the risk e.g. management may ignore risks due to flood in city like Gurgaon.
- **Control Activities**: Management implements policies and procedures throughout the organization, at all levels and in all functions, to help ensure that risk responses are properly executed.
- **Information and Communication:** The organization identifies, captures and communicates pertinent information from internal and external sources in a form and timeframe that enables 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.

- **Monitoring:** Ongoing activities and/or separate evaluations assess both the presence and functioning of enterprise risk management components and the quality of their performance over time. The thought process underlying the above framework works in the following manner: For any given objective, such as operations, management must evaluate the eight components of ERM at the appropriate level, such as the entity or business unit level

4.2 Three line of defense

The three lines of defense framework and example risk appetite framework activities