
Jindal SAW Limited

Risk Management Policy

About Jindal SAW Limited

Jindal SAW Ltd. is a part of O.P. Jindal Group, one of the country's top most industry houses and the foremost indigenous steel producers and exporters. It 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 steel seamless pipes and tubes manufactured by conical piercing process used for industrial applications; Ductile iron (DI) pipes for water and wastewater transportation; and Iron ore pellets used in iron making processes like modern blast furnace process, COREX, sponge iron or DRI making etc.

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 Nanakapaya in Gujrat; Nashik and Nagothane in Maharashtra; Indore in Madhya Pradesh; Bellary in Karnataka; Kosi Kalan in Uttar Pradesh and Bhilwara in Rajasthan, with Corporate Office in Delhi.

Additionally, the plant related to DI fittings and Stainless steel pipes are taken on lease by Jindal SAW Ltd. based at Pune-Maharashtra and Kosi respectively.

Contents

1.1 Objectives.....	4
1.2 Requirement as per Companies Act, 2013	4
1.3 Requirement of Regulation 21 of the Listing Regulations	4
1.4 Definitions	5
2. Risk Organization Structure	6
3. Risk Management Framework	9
3.1 Process	9
3.2 Steps in Risk Management	9
3.2.1 Risk Identification.....	9
3.2.2 Risk Assessment.....	9
3.2.3 Risk Analysis.....	10
3.2.4 Risk Treatment - Mitigation.....	10
3.2.5 Control and Monitoring Mechanism.....	11
3.3. Risk Reporting.....	11
3.3.1. Identification of new and emerging risks / review of existing risks.....	11
3.3.2. Risk reporting of adverse event.....	12
3.4. Board's responsibility statement.....	12
3.5. Internal Audit (IA)	13
4.1. COSO Guidelines (<i>extract for reference</i>).....	14
4.1.1. The Objective Dimension.....	14
4.1.2 The Framework Component Dimension	14
4.2 Three line of defense	16
5. Appendixes.....	17
5.1 Impact Rating.....	Error! Bookmark not defined.
5.2 Likelihood Rating	Error! Bookmark not defined.
5.3 Risk Register Template.....	17
5.4 Key departments and risks	17
5.5 Document Change History and Revision Control	18
5.6 Risk Identification Form	19
5.7 Event Recording Register	20
5.8 Risk Alert Form	20

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.

APPLICABILITY

- This Policy applies to all areas of the Company's operations.

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 Regulation 21 of the Listing Regulations

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 that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls). The risk management process focuses on areas of high inherent risk, with these documented in the Risk Register.

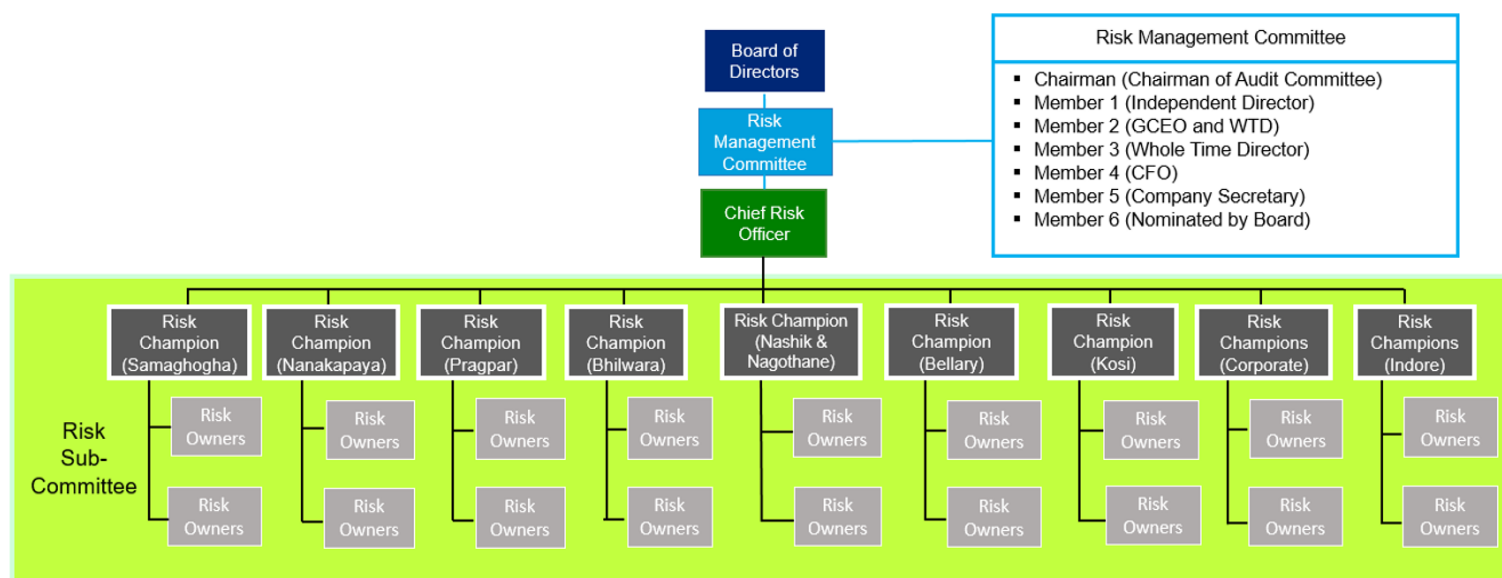
Residual Risks: Upon implementation of treatments there will still be a degree of residual (or remaining) risk, with the expectation that an unacceptable level of residual risk would remain only in exceptional circumstances.

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

The words and expressions used in this Policy but not defined herein shall have the same meaning prescribed to them in the Companies Act, 2013, Rules made thereunder, SEBI Act 1992 or Rules and Regulations made thereunder, Listing Regulations or any other relevant legislation / law applicable to the Company.

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
Board of Directors	As per the listing regulation and Companies Act, 2013	<ul style="list-style-type: none"> * The Company's risk management architecture is overseen by the Board of Directors (BOD) and policies to manage risks are approved by the Board * Ensure that the organization has proper risk management framework * Define the risk strategy and risk appetite for the company * Approve various risk management policies including the code of conduct and ethics * Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks 	

	Constitution	Roles and responsibilities	Accountable to
Risk Management Committee (RMC)	<p>* Constituted with approval of Board; The majority of members of Risk Management Committee shall consist of members of the board of directors.</p> <p>The Chairperson of the Risk management committee shall be a member of the board of directors and senior executives of the listed entity may be members of the committee.</p> <p>* The Board of Directors shall decide optimum combination of members: - chairperson shall be a member of the Board of Directors of the Company - an Independent Director, - Group Chief Executive Officer ("GCEO") and Whole Time Director ("WTD"), - Whole Time Director - Chief Finance Officer, - Company Secretary, - any member nominated by the Board.</p>	<p>* To frame, implement and monitor the Risk Management Plan for the Company.</p> <p>* To ensure that the Risk Management Policy is being followed and effectively contributing to early identification of risks and proper mitigation process.</p> <p>* Will review and approve list of risk identified, risk treatment and control mechanism.</p>	Board of Directors
Chief Risk Officer (CRO)	<p>* CRO shall be nominated by the Board, * CRO shall be supported by Risk Sub Committee</p>	<p>* To coordinate meeting of RMC at least once in a year.</p> <p>* 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.</p> <p>* To circulate Agenda for the RMC meeting.</p> <p>* To attend all RMC meetings.</p> <p>* To maintain, minutes of all RMC meetings</p> <p>* All key risks identified shall be documented in the Consolidated Risk Register maintained by Chief Risk Officer.</p> <p>* To propose periodic updates in risk management policy.</p>	Risk Management Committee
Risk Sub Committee (RSC)	<p>* Shall be formed at each location of operations viz. Corporate Office, Pragpar, Samaghogha, Nanakapaya, Nashik, Bhilwara, Kosi, and Bellary.</p> <p>* RSC(s), shall comprise of Risk Champion, and Risk Owners.</p>	<p>* It will evaluate the risk and mitigation plan recommended by Risk Owners.</p> <p>* Risk Sub Committee to hold its meeting at least once every month starting from October 2015.</p>	Risk Management Committee

	Constitution	Roles and responsibilities	Accountable to
Risk Champion (RC)	<ul style="list-style-type: none"> * 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. 	<ul style="list-style-type: none"> * 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 Owners	<ul style="list-style-type: none"> * Risk Owners shall be nominated by Risk Champions, * Each of the department shall be represented by a Risk Owner. <p>List of departments: For detailed refer to Appendix 5.4</p>	<ul style="list-style-type: none"> * 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 criticality 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 and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and 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, 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 been 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, 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” criticality may go into risk mitigation planning and implementation; low and medium critical 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.

- Once the top or critical risks are prioritized, appropriate risk mitigation and management efforts to effectively manage these risks are identified.
- Risk mitigation strategy usually involves identifying a range of options for treating risk, assessing those options, preparing and implementing risk treatment plans. The risk mitigation strategies may include managing the risk through implementation of new internal controls, accepting certain risks, taking insurance, and finally avoiding certain activities that result in unacceptable risks.
- Proposed actions to eliminate, reduce or manage each material risk will be considered and agreed as part of the Risk Assessment Workshops or as part of Management/Risk Committee.

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.

Internal Controls and Risk Management

Individual Business Units are responsible, along with support from Risk Management and other support functions, for establishing effective internal controls within various business processes. Effective design and implementation of the internal control framework is validated by regular internal audits and test of controls for these units.

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. Risk Reporting

3.3.1. Identification of new and emerging risks / review of existing risks

3.3.1.1 Risks to be reported to the Board of Directors

While the Company will be monitoring, evaluating and responding to risks. Only significant risks (or those that could become significant) need to be reported to the Board of Directors.

Significant risks include those risks that have a high likelihood or significant impact (i.e. having risk exposure 15 or more) or where there is limited ability for mitigation by the Company. These risks are identified and assessed based on the Company's expertise, judgement and knowledge.

Risks with high risk score or exposure rating will be identified and summarized in Consolidated Risk Register.

Risk Management Officer will place Consolidated Risk Register to the Audit Committee and Risk Management Committee. However, Risk Management Officer can present all the identified risk to the Audit Committee as per the need.

3.3.1.2 Process of risk reporting

The Risk Identification Form (RIF) (Refer Appendix 5.5) will be used to highlight emerging risks or add new risks to the risk register throughout the year. On an ongoing basis, when a new or emerging risk is identified, Risk owners of respective department will notify to Risk Champion by submitting the RIF.

A copy of RIF should also be mailed to designated mail id of Chief Risk Officer for discussion and inclusion in the Risk Registers. After submission of RIF, the form will be assigned a unique number which will be communicated back to the Risk Owners via acknowledgement of receipt.

RIF will be reviewed by concerned Risk Champion for evaluation. Post approval of RIF by Risk Champion, it is sent to Chief Risk Officer by Risk Champion for including it in the risk register.

After review of the RIF and in consultation with Risk Champion, Chief Risk Officer will determine whether the risk contained in this report warrants inclusion in the risk register.

Risk included in risk register in the quarter will be reported to Risk Management Committee (RMC) in the quarterly meeting.

3.3.2. Risk reporting of adverse event

All adverse events and near misses must be recorded in Event Recording Register. Details will be captured as per format in Appendix 5.6.

The adverse event reporting form (Risk alert Form) should be completed as soon as possible after the event, within one working day, unless there are exceptional reasons for delay, for example the event was identified retrospectively following a complaint or claim. All adverse events, as may be decided as significant by risk owner in consultation with risk champion, should be reported, even if some time has passed since the event occurred. The final decision of an adverse event to be reportable or not lies with the Chief Risk Officer.

It is imperative that person(s) reporting the adverse event reports the fact. There is no place for any opinion or assumptions. It is important that details are accurate and factual for any future review.

Risk owners will present the adverse event reporting form to the Chief Risk Officer immediately.

For Risk Alert format refer Appendix 5.7

Following will be the reporting mechanism:

- **To Chief Risk Officer:** The adverse events as may be jointly decided by two Risk owners (out of which one will be other department) as significant.
- **To Risk Management Committee / Board of Directors:** Adverse events with very high risk impact rating 5.

3.4. 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 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 Group Chief Executive Officer (GCEO) and the Chief Financial Officer (CFO) shall provide quarterly a statement to the Board in writing, that the financial results do not contain any false or misleading statement or figures and do not omit any material fact which may make the statements or figures contained therein misleading.

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.

3.5. Internal Audit (IA)

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

The GCEO in addition to their general and specific responsibilities, be 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 management for action and to the 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

Board of Directors			
Role	1 st line of defense	2 nd line of defense	3 rd line of defense
	Business unit	Risk management	Internal audit
Example responsibilities	Take and manage risk	Set risk policy and monitor	Validate
	<ul style="list-style-type: none"> • Conduct business in accordance with agreed strategy and related risk appetite and limits • Promote a strong risk culture and sustainable risk-return decision-making • Establish and operate business unit risk and control structure able to ensure operation within agreed policies and risk limits • Conduct rigorous self-testing against established policies, procedures, and limits • Perform thoughtful, periodic risk self-assessments • Report and escalate risk limits breaches 	<ul style="list-style-type: none"> • Establish risk management policies and procedures, methodologies and tools, including risk appetite framework, and make available throughout enterprise • Facilitate establishment of risk appetite statement with input from senior management and the board and approval of the board and set risk limits • Monitor risk limits and communicate with the CEO and the board regarding exceptions • Provide independent risk oversight across all risk types, business units, and locations 	<ul style="list-style-type: none"> • Perform independent testing and assess whether the risk appetite framework, risk policies, risk procedures, and related controls are functioning as intended • Perform independent testing and validation of business unit risk and control elements • Provide assurance to management and the board related to the quality and effectiveness of the risk management program, including risk appetite processes

Source: Deloitte Analysis. Copyright © 2014 Deloitte Development LLC.

5. Appendixes

5.1 Risk Register Template

The Management has established a template for each section to develop their Risk Register. The template could be viewed as a single sheet, which shows the following fields (or headings). Completion of the Risk Register in below format will allow review by senior management.

- Risk Identification Number
- Risk Category (Financial, Operational, Knowledge, or Strategic) *(as defined in Standard of Internal Audit (SIA) 13 issued by the Institute of Internal Auditors)*
- Risk Title
- Risk Statement (a short description of the foreseeable risk)
- Likelihood rating (estimate of likelihood of occurrence)
- Impact rating (potential consequence to people, the environment and/or Company operations etc.)
- Current mitigation plan
- Action Plan (for residual risk)
- Risk Champion and Risk Owners

Risk Identification				Risk Assessment							
Risk ID	Risk Category	Risk Title	Risk Statement	Current Mitigation Plan	Likelihood rating	Impact rating	Exposure ratings	Action Plan	Target Date	Risk Champion	Risk Owner

5.2 Key departments and risks

The Company has identified following departments:

Department wise risk summary:

S. No.	Department Categorization	No. of Risks
1	Large Diameter Business Unit	<i>Refer respective risk register</i>
2	Ductile Iron Business Unit	<i>Refer respective risk register</i>
3	Seamless Business Unit	<i>Refer respective risk register</i>
4	Pellet Business Unit	<i>Refer respective risk register</i>
5	Accounts and Taxation	<i>Refer respective risk register</i>
6	Treasury and Insurance	<i>Refer respective risk register</i>
7	Human Resource and Payroll	<i>Refer respective risk register</i>
8	Administration	<i>Refer respective risk register</i>
9	Statutory Compliances	<i>Refer respective risk register</i>
10	Projects	<i>Refer respective risk register</i>
11	Purchase (Non Raw Material)	<i>Refer respective risk register</i>
12	Inventory (Non Raw Material)	<i>Refer respective risk register</i>
13	Scrap Disposal and Logistics	<i>Refer respective risk register</i>
14	Corporate MIS and Strategy	<i>Refer respective risk register</i>
15	Kosi	<i>Refer respective risk register</i>
16	Bellary	<i>Refer respective risk register</i>
17	Information Technology (Cyber Security)	<i>Refer respective risk register</i>

5.3 Document Change History and Revision Control

The history of modifications and changes to this document are reflected in this section. All changes, updates, revisions, or comments should be documented and reflected in this section.

Date Approved:

Effective Date:

Last Reviewed:

Next Review:

Version	Sections Revised	Description of Revisions	Changed By	Date

5.4 Risk Identification Form

Risk Identification Form

Assessment No.

Brief outline of Activity or work		Assessor	
Location		Reviewed by:	

Risk Identified	Who Might be at risk	Existing Controls	Likelihood	Severity	Residual Risk	Additional Control Measures Required	Date Actioned	Estimated Residual Risk

REVIEW DATE

5.5 Event Recording Register

Event Recording register

Sr. No.	Date of occurrence of event	Nature of event	Whether the event already identified in Risk Register, if yes		Risk Treatment - Mitigation (Terminate, Treat, Transfer, Accept)	Action taken to mitigate or reduce the risk	Actual impact on the Company	Date of reporting of risk, if any
			Risk Reference no.	Mitigation plan				

5.6 Risk Alert Form

RISK ALERT		Subject		YYYY/MM/DD 1st Report
TO:				
cc:				
		Company name (abbreviation)	Reporter (Risk Management Officer)	
Date of Occurrence				
Event occurred / which may occur				
The sequence of Event (briefly)				
Content of Violating act				
Law supporting Violating act				
Influence / Penalty (including worst scenario)				
Possible Causes				
Urgent Countermeasures				
Expert Comments and Reasons (if already got)				

*If you have detailed information, please attach it separately.